Schertz Police Department

ELDERLY FRAUD RESOURCE GUIDE

Empowering older adults with the knowledge and resources needed to recognize scams, protect personal information, and prevent fraud.





SCHERTZ POLICE TEXAS

COMMON SCAMS TARGETING OLDER ADULTS

Imposter Scams
Imposter scams involve fraudsters pretending to be someone you trust, such as a government official, family member, friend, financial institution representative, or tech support representative. These scammers often use "spoofed" phone numbers, emails, or mail flyers, which make their communications appear to come from legitimate government, financial institution, or business sources. They may also use artificial intelligence (A.I.) to imitate the voices of loved ones or friends, making their calls sound convincing. Their goal is to deceive you into providing money or personal information.

Cryptocurrency Scams
Cryptocurrency is a digital payment system that does not rely on banks to verify transactions. Many common scams encourage victims to exchange money for cryptocurrency, using online trading sites or crypto ATMs. Once the cryptocurrency is sent, it is nearly impossible to track or recover. The scammers then defraud victims of the cryptocurrency.

Employment Scams
Job seekers are lured with false promises of lucrative work opportunities. Scammers often request personal information or upfront payment for training or equipment. Sophisticated scammers often create fake websites and emails that closely resemble trusted brands and businesses.

Gift Card Scams
Criminals deceive victims into purchasing gift cards under the pretext of urgent situations or fake offers. The scammer then asks the victim to provide the gift card number and PIN. Remember, gift cards are for gifts and not payments.

Home Repair/Contractor Scams
Scammers offer affordable home repair services. After receiving payment, the scammer performs subpar work or disappears.

Investment Schemes
Scammers lure victims into investing in fraudulent or non-existent opportunities, promising high returns with little or no risk.

Grandparent Scams
Scammers trick older adults into thinking they are being contacted by a grandchild or younger relative. They typically say they have a problem and need money. Verify the caller's identity with another family member, or use code names or knicknames.

Jury Duty Scams
Scammers pose as law enforcement and threaten you with fines and/or jail time for failing to comply with jury service.

Romance and Friendship Scams
Criminals adopt a fake online identity to gain a victim's affection and/or trust. The scammer then uses the illusion of a romantic or close relationship to manipulate and/or steal from the victim.

Sweepstakes/Lottery & Inheritance Scams
Scammers often claim you have won a lottery, sweepstakes, or an inheritance from an unknown relative. They may ask you to pay taxes or fees for shipping and handling, or request your account information to claim the prize.

Spousal Death & Funeral Scams
Scammers target grieving family members through obituaries and claim the deceased owes a debt that the estate must pay. The scammer offers sympathy, earns the victim's trust, and defrauds the victim of money or personal information. Imposters also pose as funeral home employees and threaten to cancel the funeral unless the victim pays more money immediately.

Tech Support Imposter Scams
Scammers often call or send fake security pop-up messages claiming that your device has a virus or that your accounts have been hacked. They trick you into providing remote access, money, passwords, or personal information.

Telemarketing & Robocall Scams
Most telemarketing scams bypass the Do Not Call registry using robocalls and prerecorded messages. These scams use spoofing to falsify the caller ID display. Examples include debt relief and credit repair scams, extended car warranties, and charity scams.

Theft by a Family/Caregiver
Distant or estranged relatives and acquaintances of elderly victims exploit their trust and love to take advantage of them and obtain their money.

THE FIVE "Ps" OF FRAUD

Scams typically involve these "P's": Pretend, Problem, Prize, Pressure, and Payment.



Scammers PRETEND to be from an organization you know.
Scammers might say they are contacting you on behalf of the government, such as the Social Security Administration, IRS, FTC, law enforcement, or Medicare. Some pretend to be from a business you know, like a utility company, a tech company, or a charity. They use spoofing to change the phone number on your caller ID. The name and number you see might not be real.

Scammers say there's a PROBLEM.
They might say you're in trouble with the government, owe money, someone in your family had an emergency, or there's a virus on your computer. Some say there's a problem with one of your financial accounts and that you must verify information.

Scammers say you've won a PRIZE.
Scammers claim that you've won a lottery or sweepstakes, but they will ask you to pay taxes or a shipping/handling fee. There is absolutely no reason to pay for a prize. Never provide your personal information or credit card number to claim a prize.

Scammers PRESSURE you to act immediately.
Scammers want you to act before you have time to think. They may insist that you not hang up the phone. The scammer might threaten to arrest or sue you, revoke your driver's license, or take your social security payments. They might say your computer is about to be corrupted with pornography or incriminating evidence.

Scammers tell you to PAY in a specific way.
They often insist you must pay using cryptocurrency, gold bars, gift cards, a payment app, or wiring money through a company like Money Gram or Western Union. Some will send you a check (that will later turn out to be fake), then tell you to deposit it and send them money. Some scammers also instruct victims to withdraw large amounts of cash and give it to a "courier" for pickup.

PHISHING MESSAGES

Phishing occurs when a scammer, masquerading as a trusted entity, tricks a victim into opening an email, clicking on a pop-up message, or responding to a text or social media message.

Common Indicators of Phishing

- Offers that seem too good to be true
- High-pressure sales pitches that stress urgency
- Alerts that there is a problem with an account
- Shortened or misspelled links
- Emails that don't address you by name
- Messages with poor grammar and spelling
- Direct requests or demands for payment
- Requests to confirm personal information

AVOIDING TELEMARKETING SCAMS

- Never send money or give out personal information such as credit card numbers, bank account numbers, birthdays, or Social Security numbers to unknown individuals
- Research unfamiliar businesses and services
- Request documentation about an offer or charity
- Do not be pressured into making a decision or payment
- Never pay for a "free prize"
- Pay for services only after they are delivered
- Understand that your personal information is often brokered through third parties







PROTECT YOURSELF FROM FRAUD

Stop Mail Fraud At The Mailbox
USPS Informed Delivery is a free service that prevents mail theft by emailing you photos of your letter-size mail. Promptly collect your mail.

Halt Scammers At Your Door
Install a doorbell camera. Don't answer the door if you don't recognize a visitor. Have a refusal script handy if you are pressured to buy or donate.

Prevent Garbage Theft
Shred receipts, credit offers, loan and credit applications, insurance forms, bank statements, and similar documents when you no longer need them.

Audit Your Wallet
Leave your Social Security card and Medicare card at home – unless you are going to need them for a specific reason.

Watch For Credit Card Skimming
Skimmers capture data from the magnetic stripe on credit cards. Use contactless payment methods when possible.

Protect Your Financial Accounts
Every few months, revise the passwords on your financial accounts. Consider using a passphrase - a short sentence you'll easily remember. Keep track of passwords in a secure password manager.

Secure Your Computer
Turn on two-factor authentication for secure websites. Use an anti-virus software service. Paid subscriptions include ad tracker blocking, cloud backups, and identity theft monitoring.

Protect Your Email Accounts
Designate unsolicited and unwanted emails in your inbox as spam to block future emails. Do not open file attachments in emails from businesses or people you don't trust completely.

Safeguard Your Smartphone
If you have a newer phone, turn on biometric identification (fingerprint or facial recognition). Set up your phone to send calls from unknown numbers to voicemail. Sign out of apps for credit cards, banks, and payment apps, including Venmo or Zelle, when you aren't using them.

Set Limits on Social Media
Scammers use social media to target individuals. If your Facebook profile photo shows you with your children or grandchildren, they might pose as them. To protect your privacy, adjust your settings so only friends can see your profile. Click the arrow in the upper-right corner, go to "Settings & Privacy," then "Privacy Checkup." Also, avoid accepting friend requests or replying to messages from unknown individuals.

Verify Online Stores
Check the spelling of websites. Scammers often create a URL with one letter off from the authentic one and hope you won't catch it. Remove credit card information from restaurant delivery and retail sites. Pay using a secure e-payment service.

Monitor Your Credit Cards And Bank Accounts
Enable mobile alerts for your credit card to receive real-time notifications for purchases. Regularly review your credit card statements for unauthorized activity and report unusual transactions to your financial institution. Set up alerts based on specific transaction thresholds. Use a gel pen when writing checks. Build a relationship with your banker to keep your finances on track and have a reliable source to turn to if any issues arise with your accounts.

PROTECT YOUR LOVED ONES FROM SCAMS

Scams and fraud by strangers can happen even in protected places like assisted living communities and nursing homes.

Signs To Look For

- A large amount of money is missing from their bank account(s)
- Numerous withdrawals of smaller amounts, such as $100 at a time
- A large check written to someone you do not know
- A change in power of attorney or insurance/investment beneficiaries
- Bounced checks or unpaid bills
- Unusual or unnecessary purchases or home repairs
- A caregiver or “friend” who is overly interested in the older adult’s finances or blocks access to them
- Piled up sweepstakes, mailings, magazine subscriptions, or “free gifts”
- Numerous phone calls or messages from suspicious people

MENTAL AND EMOTIONAL EFFECTS OF FRAUD

Victims of scams may experience a variety of mental and physical effects, including anger, anxiety, depression, embarrassment, grief, loss of confidence, reluctance to accept that it was a scam, shame, stress, and trouble sleeping.

If you are a scam victim, it is important to remember you are not alone. Don’t be ashamed to report the crime or to ask for emotional support from family, a trusted person, doctor, or a mental health counselor.





REPORTING SUSPECTED FRAUD

Contact Your Bank

- Contact your bank(s) immediately and ask for the fraud department. Tell them you plan to file a police report.
- Close your debit and credit card accounts and ask for new cards.
- If necessary, ask for a new checking account.
- Request recent bank statements or obtain them online.
- Check bank statements for transactions you didn't make.
- If you receive documents from your bank, follow-up quickly. Some banks have time thresholds for investigations.

Contact Police

- Notify your local police department that you are a fraud victim.
- Request a report number to provide to your bank(s) and credit bureau.
- Be prepared to give police a copy of your bank statements.
- Don't assume your case will be solved quickly. Investigations may take months or years, and suspects may not be apprehended.

Contact Credit Bureaus

- Contact all three credit bureaus to place a fraud alert. A fraud alert is free - and will make it harder for someone to open new accounts in your name.
- Freeze your credit to prevent scammers from opening new credit cards or making purchases in your name. You can unfreeze it as needed for legitimate transactions.

MONITOR YOUR CREDIT REPORT

Free online credit reports are available from Equifax, Experian and TransUnion. The reports are available at AnnualCreditReport.com - the only source for free credit reports authorized by Federal law.

EXPERIAN
1-888-EXPERIAN (1-888-397-3742)
www.Experian.com/fraudalert

EQUIFAX
1-888-766-0008
www.Equifax.com/CreditReportAssistance

TRANSUNION
1-800-680-7289
www.TransUnion.com/fraud

RESOURCE GUIDE

There are a number of ways to report fraud at the local, state, and national levels. The Federal Trade Commission (FTC) provides several online reporting tools for a variety of fraud. If you are unsure of what type of fraud to report, use the "Report Fraud" website below.

ReportFraud.ftc.gov

AARP
AARP's Fraud Helpline is a free resource for AARP members and non-members, staffed by trained fraud specialists and volunteers.
- 1-877-908-3360

Do Not Call Registry
- 1-888-382-1222 or 1-866-290-4236 (TTY)
- donotcall.gov

Identity Theft
Create an Identity Theft Report by filing a report with the FTC. Your Identity Theft Report proves to businesses that someone stole your identity, and makes it easier to correct problems cause by identity theft.
- Identitytheft.gov
- 1-877-438-4338

Internet Crime Complaint Center (IC3)
File complaints about online crimes including cryptocurrency schemes, ID theft, credit card fraud, ransomware, business email compromise scams, financial fraud, romance scams, lottery/ sweepstakes scams, and more.
- ic3.gov

Social Security Related Scams
Report suspected Social Security fraud or scams contact the Office of the Inspector General of the Social Security Administration. This includes suspicious calls, letters, texts, or emails about an alleged problem with your Social Security number, account, or payments.
- 1-800-772-1213 or 1-800-325-0778 (TTY)
- ssa.gov/scam
- oig.ssa.gov

If your Social Security card was lost or stolen, you can apply online for a free replacement card:
- ssa.gov/ssnumber

U.S. Securities and Exchange Commission (SEC)
If you have a question or concern about an investment or believe you have encountered fraud, contact the SEC or Financial Industry Regulatory Authority (FINRA).
- investor.gov
- SEC: 1-800-732-0330
- FINRA Complaints and Tips: 1-301-590-6500

National Elder Fraud Hotline
- 833–FRAUD–11 or 833–372–8311

Texas State Attorney General Scam Reporting
Learn about emerging scams or file a scam complaint.
- texasattorneygeneral.gov/consumer-protection
- 800-621-0508

Texas Elder Justice Coalition
- txelderjustice.org
- 682-235-5354

Adult Protective Services (APS)
Report suspected abuse, neglect, or financial exploitation of an older adult or adult with a disability. Reports can be made 24 hours a day by phone or online.
- 1-800-252-5400
- dfps.texas.gov/adult_protection

1400 Schertz Parkway, Bldg. 6
Schertz, TX 78154

210-619-1200
Schertz.com/Police

@schertzpolice
Schertz Police Department