



# Financial Scam Warning Signs

Fraudsters are constantly evolving their tactics to target vulnerable individuals, particularly seniors. This comprehensive guide covers major scam categories including bank/government impersonation, tax/SSA, Medicare, refund & overpayment, investment & crypto, property/real-estate, tech support, and romance/grandparent scams. Each section highlights clear red flags and provides actionable steps to protect yourself. According to the FBI's 2024 data, reported internet-crime losses in the U.S. reached a staggering **\$16.6 billion**, with seniors (60+) reporting **\$4.885 billion** in losses. Investment fraud leads all categories, while tech-support scams and real-estate fraud remain significant threats.



# How Scammers Target Seniors

Seniors have become prime targets for sophisticated scammers who exploit specific vulnerabilities. Understanding why older adults are particularly susceptible is the first step in building effective defenses against these predatory tactics.

## Trust & Politeness

Seniors often come from generations that value courtesy and respect for authority figures. This makes it psychologically more difficult for them to hang up on someone claiming to be an "official" or to question the legitimacy of someone who sounds professional and authoritative.

## Financial Stability

Retirement savings, home equity, and accumulated wealth make seniors attractive targets. Criminals know that older adults often have access to substantial financial resources built over a lifetime, creating a lucrative opportunity for fraudsters.

## Isolation

Many seniors experience social isolation, which reduces their opportunity to get second opinions about suspicious contacts. This isolation creates vulnerability that scammers exploit by building false relationships and positioning themselves as trusted advisors or companions.

## High-Pressure Scripts

Scammers use carefully crafted scripts designed to create a sense of urgency, fear, and secrecy. These psychological manipulation tactics are particularly effective against individuals who may be less familiar with how modern scams operate.

The targeting of seniors has intensified significantly in recent years. According to 2024 data, elder-fraud complaints and associated financial losses have **jumped approximately 46% and 43% year-over-year**, respectively. This alarming trend underscores the critical importance of education and vigilance among older adults and their support networks.

Scammers continuously refine their approaches, studying the psychological vulnerabilities of their targets and adapting their tactics to exploit trust and create emotional responses that override rational decision-making. By understanding these targeting methods, seniors and their families can better recognize when they're being manipulated and take appropriate protective actions.



# Bank & Government Impersonation

Government and financial institution impersonation scams represent some of the most common and financially devastating frauds targeting seniors. These scams leverage the authority and trust associated with organizations like the IRS, Social Security Administration (SSA), and Medicare to create a false sense of urgency and fear.

## Red Flags

- Unsolicited calls claiming your account or benefits are **suspended** and requiring immediate action
- Requests to confirm or provide one-time passwords (OTPs) or PINs over the phone
- Demands to move money to a supposedly **"safe"** account to protect it from fraud
- Instructions to purchase gift cards, cryptocurrency, or gold as a form of payment
- Threats of arrest, legal action, or benefit termination if you don't comply immediately
- Callers who insist on staying on the phone while you follow their instructions

## Do This Instead

- **Hang up immediately** - remember that caller ID can be easily spoofed
- Call the number printed on your **bank card** or visit the **official SSA/IRS website** to find legitimate contact information
- Report the scam attempt to the actual organization being impersonated
- Never share personal information, account details, or verification codes with unsolicited callers

Scammers often create elaborate scenarios designed to trigger emotional responses. They may claim your Social Security number has been compromised in criminal activity, that your Medicare benefits are about to be terminated, or that you owe back taxes that must be paid immediately. These high-pressure tactics aim to short-circuit your critical thinking and push you toward hasty decisions.

Remember that legitimate government agencies and financial institutions will never demand immediate payment via unusual methods like gift cards or cryptocurrency. They also won't threaten immediate arrest or benefit termination during an initial contact. When in doubt, independently verify the contact through official channels before taking any action.



⚠ The SSA Office of Inspector General reports ongoing SSA impostor letters, calls, and texts targeting beneficiaries. **Never use phone numbers provided in suspicious messages** - always go directly to the official SSA website or call the verified number on your statements.

"Government agencies will never call you demanding immediate payment or personal information. They typically communicate through official letters sent via postal mail."



# Tax & Medicare Scams

Tax and Medicare scams represent specialized forms of government impersonation that target specific vulnerabilities around healthcare concerns and tax obligations. These scams often spike during tax season or Medicare enrollment periods but can occur year-round.



## Tax Scam Tactics

Scammers claim to represent the IRS, offering "instant tax rebates" or threatening immediate legal action for supposed tax delinquency. They create false urgency by claiming you must act immediately to receive a refund or avoid prosecution.



## Medicare Fraud Approaches

Fraudsters contact seniors claiming they need to "update Medicare cards" or verify information to continue benefits. They may offer free medical equipment or services to obtain Medicare numbers, which are then used for fraudulent billing.

## Red Flags

- Promises of "instant tax rebates" or "immediate refunds" without proper filing procedures
- Urgent requests to "update your Medicare card now" or risk losing benefits
- Demands for payment via **gift cards, wire transfers, or cryptocurrency**
- Unsolicited calls claiming to be from "Tax Department" or "Medicare Office"
- Offers of free medical equipment in exchange for your Medicare number
- Threats of arrest, deportation, or license revocation related to tax issues
- Emails with suspicious attachments claiming to be tax forms or Medicare documents
- Pressure to act immediately without consulting family or advisors

## Do This Instead



### Verify Independently

For tax matters, check only at **irs.gov** or contact your legitimate tax preparer directly. Never use contact information provided in suspicious messages.



### Consult Official Sources

For Medicare concerns, talk to your **doctor, insurer, or call Medicare** directly using the number on your Medicare card or from the official website.



### Report Suspicious Activity

Report tax scams to the Treasury Inspector General for Tax Administration and Medicare scams to 1-800-MEDICARE or the HHS Office of Inspector General.

According to the Federal Trade Commission's Consumer Advice from June 2024, Medicare numbers are increasingly valuable targets for identity thieves. These numbers can be used to submit fraudulent claims to Medicare, potentially affecting your benefits and creating administrative headaches. The FTC emphasizes that Medicare will never call you unsolicited to ask for your Medicare number.

Remember that legitimate tax refunds are processed through official channels after proper filing, and Medicare communications typically come through postal mail rather than unsolicited calls or emails. Taking time to verify before acting is your best protection against these sophisticated scams.





# Refund & Overpayment Scams

Refund and overpayment scams represent a particularly deceptive category of fraud that exploits the banking system's check processing procedures. These scams can target anyone but are especially effective against seniors who may be less familiar with how modern banking verification works.

## How It Works

### Initial Contact

The scammer contacts you regarding a purchase, service, or prize. They may pose as a company representative, lottery official, or even a potential buyer for something you're selling online.

### False Clearance

The check initially appears to clear your account, making it seem legitimate. Banks are required to make funds available quickly, but this doesn't mean the check is valid.

### The "Mistake"

They send you a check for **too much money** - often significantly more than expected. They apologize for the "error" and ask you to deposit the check and return the difference.

### The Collapse

After you've sent the "difference" (using wire transfer, gift cards, or other non-recoverable methods), the original check **bounces** - sometimes weeks later. You're now responsible for the full amount plus potential fees.

## Common Scenarios

- **Online marketplace sales:** Buyer sends check for more than your asking price, claiming it's for "shipping costs" or "movers"
- **Mystery shopper offers:** You're hired as a "secret shopper" and sent a check to buy gift cards and evaluate store service
- **Prize/lottery winnings:** You've "won" but need to pay taxes or fees from the advance check they send
- **Rental deposits:** Potential renters send excessive deposits then request partial refunds before moving in
- **Grant overpayments:** Notification that you received too much from a government grant or program
- **Refund adjustments:** Claims that a refund was calculated incorrectly and you need to return the excess

## Do This Instead

- ⊗ • **Never send money back** on an "overpayment" - insist on a new, correct payment instead
- Treat **unexpected checks** as potential scams, regardless of how official they appear
- Ask your bank to **fully verify** a check before spending any of the money - explain your concerns
- Be especially wary of any situation requiring you to **deposit a check and then send money elsewhere**
- Remember that **you are responsible** for checks you deposit that later bounce

According to the Federal Trade Commission's Consumer Advice, fake check scams continue to evolve and remain prevalent. The fundamental mechanism exploits the gap between when funds become available in your account and when a check is fully verified by the banking system. This gap creates a false sense of security that the transaction is legitimate.

The best protection is to never accept checks from unknown parties, especially those that involve returning a portion of the funds. If you must accept a check, wait at least two weeks or longer before considering the funds truly available, regardless of what your bank's funds availability policy indicates.

# Tech-Support Scams

Tech-support scams have become increasingly sophisticated, targeting seniors who may be less confident with technology. These scams exploit technical anxieties and trust in established brands to gain access to victims' devices, personal information, and financial accounts.

## Red Flags

- Pop-up windows claiming "**virus detected**" with a phone number to call for "immediate assistance"
- Unsolicited calls from people claiming to be from "Microsoft," "Apple," "Windows," or your bank's security team
- Warnings about "suspicious activity" on your computer or accounts that require immediate attention
- Requests for **remote access** to your computer to "fix problems" or "install security updates"
- Technical jargon and scare tactics about "hackers," "malware," or "compromised accounts"
- Pressure to purchase unnecessary software, services, or gift cards to resolve supposed issues

## Common Tactics

Tech support scammers typically use one of two approaches:

1. **Inbound scams:** They trick you into calling them through alarming pop-ups, fake error messages, or search engine ads that appear when looking for technical help.
2. **Outbound scams:** They call you directly, claiming to be from a reputable company, often with spoofed caller ID information to appear legitimate.

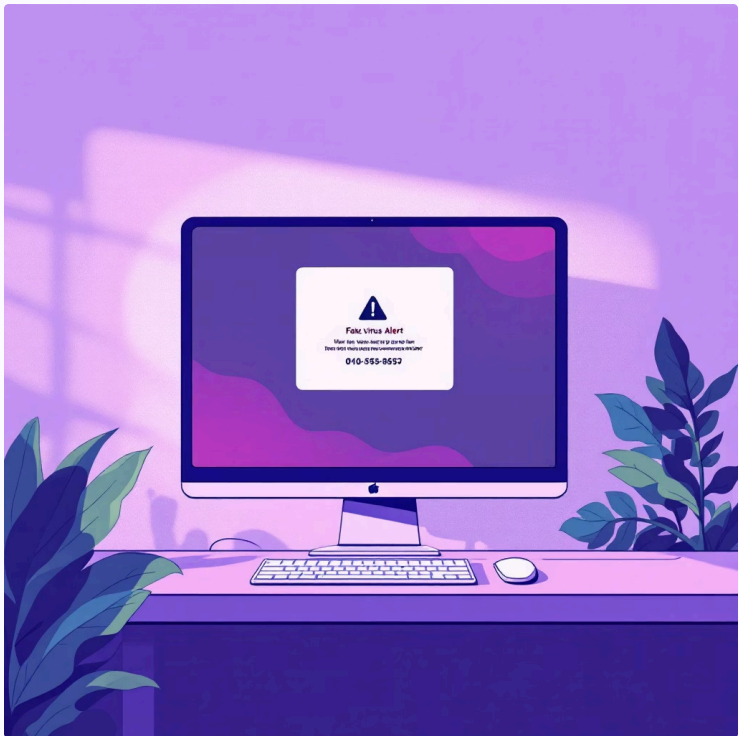
Once engaged, they use scripted "diagnostic procedures" to convince you that your device has serious problems. These might include directing you to normal system logs or benign error messages that they misrepresent as evidence of compromise.


## Do This Instead

		
<b>Force-Close</b> If you encounter alarming pop-ups, force-close your browser (use Task Manager on Windows or Force Quit on Mac). Never call numbers from pop-ups or click their buttons.	<b>Run Security Software</b> Use legitimate security software to scan your system. Most modern operating systems have built-in security tools that can perform basic scans.	<b>Contact Trusted Support</b> If you need technical help, call official support numbers found on your device, product packaging, or the company's official website (which you should access directly, not through links).

If you've already allowed remote access to your computer, disconnect from the internet immediately, run a security scan, and change all your passwords from a different, secure device. Consider having your computer professionally checked by a reputable local service provider. If you've shared financial information or made payments, contact your financial institutions immediately to report potential fraud.

Remember that legitimate technical support will never initiate unsolicited contact, use scare tactics, or request remote access without you specifically seeking assistance first. When in doubt, disconnect and seek help from trusted local resources or family members with technical expertise.



 2024 tech-support scam losses topped **\$1.46 billion** according to reported data. Older adults are heavily targeted by call-center fraud operations, which often operate internationally while appearing to be domestic.

"Legitimate tech companies will never proactively contact you about device problems, nor will they use pop-up warnings to solicit phone calls."



# Investment & Crypto Scams

Investment and cryptocurrency scams represent some of the most financially devastating frauds targeting seniors. These sophisticated schemes often combine elements of relationship manipulation with promises of extraordinary returns, creating a powerful psychological trap that can lead to substantial financial losses.

## Red Flags

### Unrealistic Promises

Claims of **"no risk, guaranteed returns"** or investment opportunities that consistently outperform legitimate market benchmarks. Legitimate investments always involve some degree of risk, and returns fluctuate with market conditions.

### Pressure Tactics

Creating artificial urgency to act quickly before an "opportunity expires" or using exclusivity claims suggesting you've been "specially selected" for a privileged investment opportunity.

### Unverifiable Platforms

Directing you to unusual, proprietary trading platforms or investment portals that aren't registered with appropriate financial authorities. These platforms often display fake profits to encourage larger investments.

### Relationship Manipulation

Building trust through romantic interest or mentorship before introducing investment opportunities. In "pig-butchering" scams, victims are "fatted up" with attention before being led to financial slaughter.

## "Pig-Butchering" Romance-Investment Scams

This particularly insidious form of fraud combines elements of romance scams with investment fraud. The process typically follows this pattern:

1. **Contact initiation:** Scammers reach out through dating apps, social media, or even wrong-number texts, establishing friendly conversation
2. **Relationship building:** They invest weeks or months building trust and emotional connection without asking for money
3. **Investment introduction:** The scammer mentions their own financial success through investments, often in cryptocurrency
4. **Guided investment:** They help you set up accounts on fraudulent platforms and guide initial small investments that appear to generate impressive returns
5. **Escalation:** Encouraged by apparent success, victims invest larger amounts, often liquidating legitimate retirement accounts
6. **Extraction:** When victims try to withdraw funds, they're told they must pay taxes, fees, or additional investments to access their money

## Do This Instead



- **Never invest** via links or platforms provided by someone you've recently met online
- **Verify advisors** through official channels like the SEC's Investment Adviser Public Disclosure database or FINRA's BrokerCheck
- **Research platforms** independently through regulatory resources, not through search results that may be manipulated
- **Consult trusted family members** or financial professionals before making investment decisions
- **Be extremely skeptical** of investment opportunities involving cryptocurrency, forex trading, or binary options presented through social channels

According to 2024 Internet Crime Complaint Center (IC3) data, investment fraud resulted in **\$6.57 billion** in reported losses overall, with cryptocurrency investment scams accounting for **\$5.8 billion** of that total. The largest age group reporting these losses was adults aged **60 and older**, highlighting the targeted nature of these scams against seniors.

Remember that legitimate investments are registered with appropriate regulatory authorities, offer transparent information about risks and returns, and never require urgent action or unusual payment methods. When considering any investment, take time to research independently and seek advice from trusted financial professionals not connected to the opportunity being presented.





# Property & Real-Estate Scams

Property and real-estate scams target one of the most significant assets many seniors possess - their homes. These sophisticated frauds can result in substantial financial losses and complex legal entanglements that may be difficult to resolve.

## Real-Estate Wire Fraud

This increasingly common scam targets home buyers and sellers during property transactions when large sums of money are being transferred.

### How It Works

1. Scammers hack into email accounts of real estate agents, title companies, or attorneys involved in property transactions
2. They monitor communications to identify upcoming closings and wire transfers
3. Just before the scheduled transfer, they send fraudulent emails with **altered wire instructions**
4. Unsuspecting buyers wire their down payment or closing funds to the scammer's account instead of the legitimate recipient
5. Once transferred, the money is quickly moved through multiple accounts and often out of the country, making recovery extremely difficult

### Protection Strategies

- Always **call your escrow agent or real estate professional** on a **known phone number** to verbally confirm wire instructions before sending funds
- Be suspicious of last-minute changes to wiring instructions or payment procedures
- Verify email addresses carefully - scammers often use addresses that look legitimate but differ by one character
- Consider using cashier's checks for closing instead of wire transfers when possible



⚠️ 2024 data shows **real-estate and rental fraud losses of \$173.6 million** reported to the Internet Crime Complaint Center. FBI field bulletins continue to warn about persistent rental-listing scams targeting both long-term housing and vacation rentals.

## Deed/Title Fraud

Also known as "home title theft," this scam involves criminals filing fraudulent documents to transfer ownership of property without the legitimate owner's knowledge.

### How It Works

1. Fraudsters identify potential targets, often focusing on properties with no mortgages, vacation homes, or properties owned by seniors
2. They **forge ownership documents** and file them with county recorders
3. Once the property appears to be in their name, they may sell it to unsuspecting buyers or take out loans using the property as collateral
4. Legitimate owners often discover the fraud only when they receive unexpected documents or when attempting to sell their property

### Protection Strategies



#### Monitor Records

Regularly check county **property records** for unexpected changes or filings related to your property. Many counties offer online access to these records.



#### Set Up Alerts

Sign up for **recorder alerts** if available in your county. These services notify you when documents are filed against your property.



#### Consider Title Insurance

Maintain owner's title insurance that includes fraud protection. Review your policy to understand what protections it provides.



#### Act Quickly

If you discover fraudulent activity, contact law enforcement, your county recorder's office, and an attorney specializing in real estate fraud immediately.

According to the Federal Trade Commission's Consumer Advice from August 2024, consumers should be skeptical of "title lock" marketing claims. The FTC emphasizes that these services don't actually "lock" your title - they primarily offer monitoring services that alert you to changes, similar to what many counties already provide for free or at minimal cost.

For rental scams, always verify property ownership through tax records, meet landlords in person when possible, and never wire money or send deposits for properties you haven't physically inspected. Be particularly wary of listings with prices significantly below market rates or landlords who claim they can't show the property in person due to being out of town or overseas.



# Romance, "Grandparent," & Family-Emergency Scams

Romance and family-emergency scams represent some of the most emotionally manipulative frauds targeting seniors. These schemes exploit deep human needs for connection and family loyalty, making them particularly devastating both financially and psychologically.

## Romance Scams

Romance scams involve creating false romantic relationships to extract money from victims. These sophisticated schemes often unfold over months, with scammers investing significant time to build trust and emotional dependency.

### How They Work

1. Scammers create attractive profiles on dating sites or social media, often impersonating military personnel, professionals working overseas, or widowed individuals
2. They engage in intensive communication, expressing deep affection quickly and creating a sense of a genuine relationship
3. After establishing emotional connection, they begin sharing "hardships" that require financial assistance
4. Common scenarios include medical emergencies, being stranded while traveling, customs fees for valuable items, or investment opportunities
5. They may promise to repay the money or visit once their "situation" improves, but always find reasons why this can't happen

### Red Flags

- Reluctance or inability to video chat or meet in person
- Professions of deep love or commitment unusually early in the relationship
- Detailed personal stories that evoke sympathy and emotional response
- **Sudden online romance asking for money or investment advice**
- Requests for financial assistance, regardless of the reason given

## Do This Instead

### Verify Identities

**Video-verify** the identity of anyone you meet online before sending money or personal information. For romance scams, insist on video calls where you can interact in real-time. Be aware that deepfake technology exists but is still difficult to maintain during extended live conversations.

### Ask Verification Questions

Ask callers claiming to be family members questions that a stranger couldn't easily answer. Avoid questions with answers that might be available on social media (like pet names or vacation spots).

## "Grandparent" & Family-Emergency Scams

These scams exploit family bonds by creating false emergencies involving loved ones, particularly targeting grandparents who may be less likely to verify the situation before responding.

### How They Work

1. Scammers call claiming to be a grandchild or other relative in trouble
2. They create scenarios involving arrests, accidents, or medical emergencies requiring immediate financial assistance
3. Often they'll say **"Grandpa/Grandma, it's me - I'm in trouble"** and let the victim supply the name
4. They may have an accomplice pose as an authority figure (lawyer, doctor, police officer) to add credibility
5. They insist on secrecy, urging the victim not to tell other family members about the situation

### Red Flags

- Requests for unusual payment methods like gift cards, wire transfers, or cryptocurrency
- Insistence on immediate action without time to think or verify
- Demands for secrecy and warnings not to contact other family members
- **"Grandson in jail — send bail now, don't tell anyone"**
- Poor call quality or background noise that makes voice identification difficult

### Contact Family Directly

For family emergencies, hang up and **call family members on known numbers** to verify the situation. Contact the person in trouble directly, even if the caller claims they can't talk. If you can't reach them, call other family members who would know about the situation.

### Resist Pressure

Legitimate emergencies rarely require immediate wire transfers or gift cards. Take time to verify the situation, regardless of how urgent it seems. Real family members will understand your need to confirm their identity.

Romance scams and family-emergency frauds are particularly effective because they target emotional vulnerabilities rather than logical decision-making. The psychological manipulation involved can make victims reluctant to question the situation or seek outside advice, especially when scammers have invested time in building trust or creating a sense of urgency.

If you've been victimized by one of these scams, report it immediately to local law enforcement, the FBI's Internet Crime Complaint Center (IC3), and the Federal Trade Commission. While financial recovery may be difficult, reporting helps authorities track patterns and potentially prevent others from becoming victims.

# Quick Reference Guide

This quick reference summarizes the key warning signs and protective responses for each major scam category. Keep this information readily accessible for yourself and share it with friends and family members who might be vulnerable to these sophisticated fraud attempts.

Scam Type	Red Flag	Safe Response
Bank/SSA/IRS Impersonation	"Benefits suspended" / OTP request / Urgent action needed	Hang up; call <b>official</b> number from your card or statement
Tax & Medicare	"Instant refund" / "Update Medicare card now"	Verify only through irs.gov or call Medicare directly
Refund/Overpayment	"We overpaid — send back difference"	Never return money from <b>unexpected checks</b>
Tech Support	Pop-ups; demands for remote access	Close browser; run security scan; call <b>trusted</b> support
Investment/Crypto	"Guaranteed returns," secret platform	Don't send money; verify advisors independently
Real-estate Wire Fraud	New wire instructions via email	Call escrow/agent on <b>known number</b>
Deed/Title Fraud	Unexpected liens/ownership changes	Monitor property records; set alerts; act quickly
Romance/Grandparent	Emotional pressure & secrecy	Video-verify; confirm with family on known numbers

## General Protection Strategies

- Never make financial decisions under pressure - legitimate organizations will give you time to think
- Verify contacts independently using official numbers from statements or websites you navigate to directly
- Be skeptical of unusual payment requests, especially gift cards, wire transfers, or cryptocurrency
- Discuss suspicious contacts with trusted family members or friends before taking action
- Keep computer security software updated and be cautious about clicking links or opening attachments

## If You've Been Scammed

- Contact your financial institutions immediately to report fraud and potentially stop payments
- Report the scam to local law enforcement and file a complaint with the FBI's Internet Crime Complaint Center (IC3)
- Report identity theft at IdentityTheft.gov if personal information was compromised
- Change passwords for any accounts that may have been accessed or compromised
- Continue to monitor financial statements and credit reports for unusual activity

Remember that scammers continuously evolve their tactics, but the fundamental red flags remain consistent: urgency, secrecy, unusual payment methods, and unsolicited contacts. By maintaining healthy skepticism and following verification procedures, you can significantly reduce your risk of becoming a victim.

The most effective protection against financial scams is a combination of awareness and a support network. Share this information with friends and family, and establish trusted contacts who can help verify suspicious situations. Creating a habit of discussing potential scams openly helps remove the stigma and secrecy that scammers rely on to isolate their victims.