FRAUD GUIDE *for Seniors*

Fraud can happen to anyone. Scammers are smart, patient, and convincing. They often use fear, urgency, kindness, romance, or confusion to get people to act before they think.

In 2025, adults age 60 and older reported more than **$7.7 billion in losses** to the FBI's Internet Crime Complaint Center, and scams targeting older adults continue to grow. Investment scams, tech support scams, romance scams, government imposter scams, and social media scams remain some of the biggest threats. *(Internet Crime Complaint Center)*

COMMON SCAMS TARGETING SENIORS

Bank Imposter Scams

A scammer may call, text, or email pretending to be your bank. They may say there is fraud on your account and ask you to "verify" your username, password, debit card number, online banking code, or one-time passcode.

WATCH FOR:

- "Your account has been locked."
- "We need your code to stop fraud."
- "Move your money to a safe account."
- "Do not tell anyone about this."

WHAT TO DO: Do not respond. Do not click the link. Call your bank using the phone number on its official website or your statement.

Government Imposter Scams

Scammers may pretend to be from Social Security, Medicare, the IRS, law enforcement, or the courts. They may say your benefits are suspended, your Social Security number was used in a crime, or you owe money.

The Social Security Administration warns that scammers use phone calls, texts, emails, social media, and even fake badges or real employee names to appear legitimate. SSA says it will never ask for sensitive personal information through social media, email, or text. *(Social Security)*

WATCH FOR:

- Threats of arrest
- Claims your benefits will stop
- Requests for payment by gift card, crypto, wire, cash, or gold
- Messages asking for your Social Security number

WHAT TO DO: Hang up. Contact the agency directly using an official government website.

Tech Support Scams

A pop-up, phone call, or email may claim your computer has a virus. The scammer may pretend to be from Microsoft, Apple, Amazon, or another trusted company. They may ask for remote access to your computer or payment to "fix" the issue. Tech support and customer support scams remain a major source of losses, especially for older adults. *(AARP)*

WATCH FOR:

- A loud warning on your screen
- A phone number telling you to call immediately
- Someone asking to control your computer
- Requests for gift cards, wire transfers, crypto, or payment apps

WHAT TO DO: Close the browser. Turn off the computer if needed. Do not call the number on the pop-up. Contact a trusted computer professional or family member.

Medicare and Health Insurance Scams

Scammers may offer "free" medical equipment, genetic testing, new Medicare cards, or health services in exchange for your Medicare number.

WATCH FOR:

- "Free" medical equipment you did not request
- Calls asking for your Medicare number
- Someone saying you need a new Medicare card immediately
- Pressure to switch plans quickly

WHAT TO DO: Do not share your Medicare number with unexpected callers. Review your Medicare statements for services you did not receive.

Investment and Cryptocurrency Scams

These scams often promise high returns with little or no risk. They may start through social media, online ads, text messages, dating apps, or even a "friend" who claims they made money.

Investment scams caused major reported losses in 2025, with the FTC reporting more than **$7.9 billion** in losses and a median individual loss of more than **$10,000**. *(Consumer Advice)*

WATCH FOR:

- "Guaranteed returns"
- "Low risk, high reward"
- Pressure to invest quickly
- Requests to use cryptocurrency
- A website or app that shows fake profits
- Someone offering to help recover money you already lost

WHAT TO DO: Pause before investing. Talk to a trusted financial professional. Be especially cautious if the opportunity came through social media or a person you have never met in real life.

Grandparent and Family Emergency Scams

A scammer pretends to be a grandchild, child, friend, police officer, lawyer, or hospital worker. They may say your loved one is in jail, injured, or in trouble and needs money immediately.

WATCH FOR:

- "Grandma, don't tell Mom and Dad."
- "I need bail money."
- "Send cash right away."
- "This is an emergency."

WHAT TO DO: Hang up. Call your loved one directly. If you cannot reach them, call another family member. Create a family code word for real emergencies.

Romance and Friendship Scams

A scammer builds trust over time, often through social media, dating sites, games, or messaging apps. Once the relationship feels real, they ask for money due to an emergency, travel issue, medical bill, business problem, or investment opportunity.

WATCH FOR:

- They cannot meet in person
- They ask to move the conversation offline
- They have sudden emergencies
- They ask for money, gift cards, crypto, or bank access
- They ask you to keep the relationship secret

WHAT TO DO: Do not send money to someone you have not met in person. Talk to someone you trust before making any financial decision.

Social Media Scams

Scammers use fake profiles, hacked accounts, ads, quizzes, marketplace listings, and messages to steal money or information. The FTC reported that people lost **$2.1 billion** to social media scams in 2025, with shopping scams, investment scams, and romance scams among the top categories. *(Federal Trade Commission)*

WATCH FOR:

- Too-good-to-be-true ads
- Friend requests from people you already know
- Messages asking for money
- Fake giveaways
- Investment tips from strangers
- Links asking you to log in

WHAT TO DO: Do not click suspicious links. Verify messages by contacting the person another way. Be careful what you share publicly.

THE GOLDEN RULE

Stop. Hang up. Don't click. Don't send money. Talk to someone you trust.

A HELPFUL PHRASE TO REMEMBER

"I don't make financial decisions under pressure."

Say it out loud. Hang up. Walk away. Call someone you trust.

Delivery, Text Message, and QR Code Scams

Scammers send texts or emails that look like USPS, UPS, FedEx, Amazon, or another delivery service. They may say a package could not be delivered and ask you to click a link or scan a QR code.

WATCH FOR:

- "Your package is delayed."
- "Confirm your address."
- "Pay a small redelivery fee."
- Links that do not look official
- QR codes in unexpected messages

WHAT TO DO: Do not click the link. Go directly to the official delivery website or app and enter the tracking number yourself.

Fake Prize, Lottery, and Sweepstakes Scams

A scammer says you won money, a car, a gift card, or a prize. Then they ask you to pay taxes, fees, or shipping before you can receive it.

WATCH FOR:

- "You won, but you must pay first."
- Requests for gift cards or wire transfers
- Claims from Publishers Clearing House or a fake charity
- Pressure to keep it secret

WHAT TO DO: Never pay money to receive a prize.

Charity and Disaster Scams

After natural disasters, tragedies, or local fundraisers, scammers create fake charities or pretend to represent real ones.

WATCH FOR:

- Pressure to donate immediately
- Vague charity names
- Requests for gift cards, cash, crypto, or wire transfers
- No clear information about how donations are used

WHAT TO DO: Donate directly through the charity's official website. Be careful with links in emails, texts, and social media posts.

Caregiver, Family, or Trusted Person Financial Exploitation

Not all fraud comes from strangers. Sometimes financial abuse involves a caregiver, family member, friend, or someone with access to an older adult's money.

WATCH FOR:

- Unexplained withdrawals
- New "friends" managing money
- Missing checks or cards
- Unpaid bills despite available funds
- Changes to wills, beneficiaries, or account access
- Someone isolating the older adult from family or friends

WHAT TO DO: Contact the bank, Adult Protective Services, local law enforcement, or a trusted professional.

RED FLAGS—SCAM WARNING SIGNS

BE CAREFUL WHEN SOMEONE:

- Asks you to act immediately
- Tells you to keep it secret
- Asks for gift cards, cryptocurrency, wire transfers, cash, or gold
- Requests your online banking username or password
- Asks for a one-time passcode
- Wants remote access to your computer
- Says you are in trouble with the government
- Claims your money must be moved to a "safe account"
- Offers guaranteed investment returns
- Sends a link you were not expecting
- Asks for personal information by text, email, or social media

WHAT TO DO IF YOU THINK YOU'VE BEEN SCAMMED

STEP 1: STOP COMMUNICATING	Do not answer more calls, texts, emails, or messages from the scammer.
STEP 2: CONTACT YOUR BANK IMMEDIATELY	Call your bank using the number on its official website, your statement, or the back of your card. The faster you act, the better chance there may be to limit damage.
STEP 3: CHANGE PASSWORDS	Change passwords for online banking, email, shopping accounts, and social media. Use strong, unique passwords.
STEP 4: TURN ON EXTRA SECURITY	Use account alerts, multifactor authentication, card controls, credit monitoring, and online banking notifications.
STEP 5: REPORT IT	Report online scams to the FBI's Internet Crime Complaint Center. The FBI says reports help investigators track trends and may help freeze stolen funds in some cases. *(Internet Crime Complaint Center)* Also report fraud to the FTC, and report Social Security scams to the Social Security Administration Office of the Inspector General. *(Social Security)*
STEP 6: SAVE EVERYTHING	Keep texts, emails, receipts, screenshots, phone numbers, websites, names used, and payment details.
STEP 7: TELL SOMEONE YOU TRUST	Scammers count on embarrassment and silence. You are not alone, and reporting quickly can help protect you and others.

SIMPLE SAFETY HABITS

- Let unknown calls go to voicemail.
- Use phone numbers from official websites.
- Do not click links in unexpected texts or emails.
- Do not give out one-time passcodes.
- Set up account alerts.
- Review bank and credit card statements often.
- Shred documents with personal information.
- Freeze your credit if you are not applying for new credit.
- Talk to a trusted contact before large withdrawals or transfers.
- Be cautious with new online friendships, investment offers, and urgent requests.

At Minster Bank, protecting your financial well-being is part of how we serve you.
If something feels unusual, urgent, or suspicious, contact us immediately at **866.646.7837**.