Preventing Senior Scams

© ADOBE STOCK

Why Seniors Are Targeted

Scams targeting seniors are a growing concern, costing older Americans billions of dollars annually.

© ADOBE STOCK

According to the FBI's Elder Fraud Report, adults aged 60 and older reported losing over $3.4 billion to fraud in 2023, an 11% increase — which as on top of a 35% increase in 2022. year. Nasdaq reported about 1 in 10 elderly Americans are scammed each year and that, in 2024, $77.7 billion of all reported global fraud was linked to senior victims. The average loss per victim was $34,000.

Seniors are targeted for several reasons, making them more vulnerable to these deceptive schemes. One major factor is financial stability. Many seniors have accumulated savings, own property or receive a steady income from pensions or Social Security. Scammers see this as an opportunity to exploit a perceived abundance of resources. Additionally, older adults may be less familiar with newer technologies, such as online banking or digital payment platforms, leaving them susceptible to phishing emails, fake tech support calls or fraudulent websites.

Cognitive decline can also play a role. While not all seniors experience memory or decision-making difficulties, those who do may find it harder to recognize scams or remember warning signs. This makes them easy targets for repeated fraud attempts.

Social isolation is another contributing factor. Scammers often prey on loneliness, using friendly conversations to gain trust before introducing fraudulent schemes. Romance scams, for instance, frequently target older adults looking for companionship.

Some of the most common scams targeting seniors include government impersonation scams, sweepstakes scams, robocall scams, tech support scams, confidence/romance scams and investment scams.

While seniors are prime targets, efforts to combat scams are increasing. Organizations like the National Council on Aging (NCOA) and the AARP Fraud Watch Network provide resources and education to help seniors recognize and avoid scams. Law enforcement agencies, including the FBI and local police departments, also work to track and prosecute fraudsters.

One effective prevention method is raising awareness among seniors and their families. Education campaigns teach seniors to identify red flags, such as unsolicited requests for personal information or high-pressure tactics demanding immediate payment. Families can play a critical role by helping older relatives monitor financial accounts and reviewing unusual transactions together.

Legislation also offers protections. For example, the Senior Safe Act of 2018 encourages financial institutions to train employees to detect elder financial abuse and report suspected scams. Additionally, the FTC and Consumer Financial Protection Bureau (CFPB) work to enforce laws and provide resources to safeguard seniors' assets.

Despite these efforts, scams targeting seniors remain a significant issue. Staying informed and vigilant is key to reducing losses. By fostering open communication and providing seniors with tools to protect themselves, communities can help shield vulnerable individuals from falling victim to fraud.

Older adults should remember: when in doubt, pause and verify. A quick check with a trusted friend or family member could prevent financial loss and emotional distress. Together, we can build a safer, more informed community for everyone.

How to Report Scams

Scams targeting seniors are a growing concern, with fraudsters using increasingly sophisticated tactics to steal money or personal information.

© ADOBE STOCK

While prevention is crucial, knowing how to report scams is just as important. Prompt reporting increases the chances of recovering lost funds and helps authorities protect others from falling victim to similar schemes.

Given how sophisticated many scammers are, don't be embarrassed if you are a victim. The scammer is the one in the wrong, not you. Don't let shame or embarrassment keep you from reporting a scam or crime.

Here's a step-by-step guide on how to recognize and report scams effectively.

RECOGNIZE THE SCAM

Before reporting, identify you've been scammed. Common signs include:

• Unsolicited contact demanding money or personal information.

• Pressure to act immediately or face consequences.

• Requests for payment via untraceable methods like wire transfers, gift cards or cryptocurrency.

• Promises of prizes, investments or services that seem too good to be true.

If you suspect a scam, trust your instincts and proceed with caution.

GATHER INFORMATION

When reporting a scam, the more details you can provide, the better. Gather:

• Names, phone numbers, email addresses or websites used by the scammer.

• Copies of emails, text messages or letters received.

• Transaction details, such as amounts paid, payment methods and dates.

• Descriptions of interactions, including what the scammer said or promised.

This documentation strengthens your case and aids investigators.

KNOW WHO TO CONTACT

Different scams require reporting to specific agencies:

• Federal Trade Commission (FTC): The FTC handles most consumer scams, including online shopping fraud, imposter scams and phishing. File a complaint at ReportFraud.ftc.gov.

• Your state attorney general's office: For scams involving businesses operating in your state, contact the consumer protection division of your state attorney general.

• Local law enforcement: If you've lost money or personal property, file a police report with your local department.

• The FBI's Internet Crime Complaint Center (IC3): Report cybercrimes, such as online scams, at ic3.gov.

• AARP Fraud Watch Network: Seniors can call their helpline at (877) 908-3360 for free support and resources.

• National Elder Fraud Hotline: The hotline is a free resource created by the U.S. Department of Justice. Case managers are assigned t those who call. These case managers help seniors through the reporting process at the federal, state and local levels. Call (833) 372-8311.

In addition to these resources, reach out to people in your community who can help. If you live in assisted living or a retirement community, talk to directors or managers who may be able to help you. Informing them helps them determine whether others in the community are also being targeted.

ACT QUICKLY

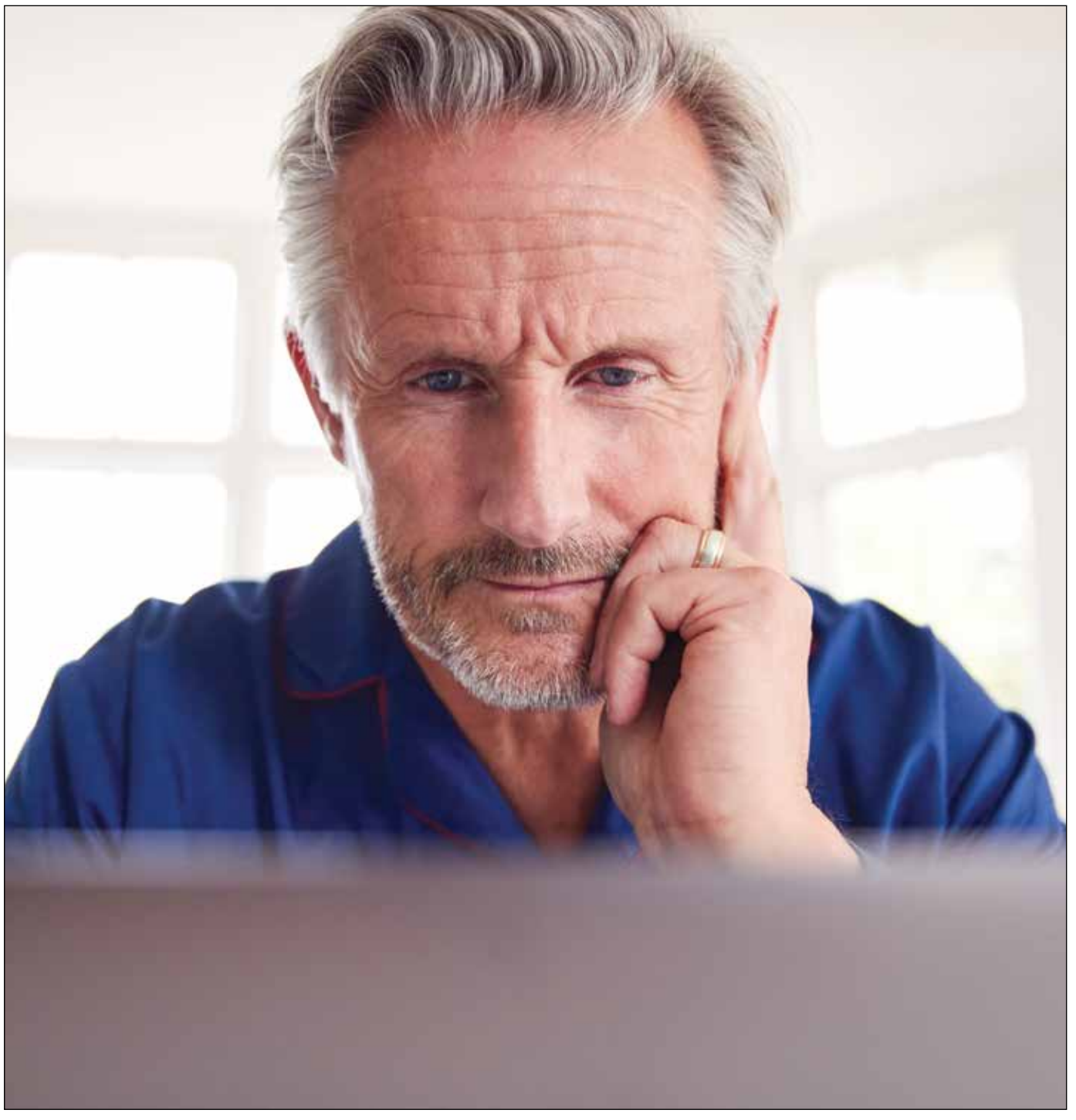
If financial loss is involved, notify your bank, credit card company or payment platform immediately to attempt reversing transactions or freezing accounts. For identity theft, visit IdentityTheft.gov to create a recovery plan.

SHARE YOUR EXPERIENCE

Scammers often target multiple people in the same community or demographic. Sharing your experience with friends, family or senior centers raises awareness and helps others avoid similar traps.

Protecting Against Modern Fraud

As cryptocurrency grows in popularity, so do scams targeting vulnerable populations, especially seniors.



© ADOBE STOCK

According to the Federal Trade Commission (FTC), seniors lost over $1.9 billion to fraud in 2023, with a significant portion tied to online payment platforms and cryptocurrency schemes. In September of 2024, the FBI released its first Cryptocurrency Fraud Report. People 60 and older filed more than 16,000 complaints of cryptocurrency fraud and reported losing more than $1.6 billion — the most of any age group tracked.

Educating seniors about these modern risks is critical to safeguarding their finances.

CRYPTOCURRENCY: A NEW FRONTIER FOR SCAMMERS

Cryptocurrency, such as Bitcoin or Ethereum, is another lucrative avenue for fraud. Seniors may encounter scams promising high returns on crypto investments or invitations to participate in initial coin offerings (ICOs) that turn out to be fraudulent.

In one common scheme, scammers pose as financial advisors, offering to help seniors invest in cryptocurrency. They may use technical jargon and flashy websites to appear legitimate. Once they've gained trust, they persuade victims to transfer funds, often through unregulated exchanges or wallets, which makes it nearly impossible to trace or recover lost money.

The FBI said the vast majority of losses were from a category they refer to as pig butchering scams. There was a 53% increase in these type of losses — from $2.57 billion in 2022 to $4 billion in 2023. That's a 53% increase from the $2.57 billion losses reported in 2022. In these scams, the criminal assumes a fake persona to create a deep relationship with the victim. During the relationship, they convince the victim to invest increasing amounts of their savings into a fake cryptocurrency investment platform.

"These schemes offer individuals large returns with the promise of minimal risk," the FBI said in the report. "Over the years, cryptocurrency's widespread promotion as an investment vehicle, combined with a mindset associated with the 'fear of missing out,' has led to opportunities for criminals to target consumers and retail investors — particularly those who seek to profit from investing but are unfamiliar with the technology and the attendant risks."

EDUCATING SENIORS ABOUT RISKS

Education is the first line of defense. Seniors need to understand the warning signs of these scams, including:

- Urgent payment requests: Legitimate companies and individuals rarely demand immediate payments via apps or cryptocurrency.
- Unsolicited offers: Be cautious of unsolicited investment opportunities or messages claiming a problem with a payment account.
- Pressure to keep secrets: Scammers often advise victims not to consult others about the transaction.
- Requests for cryptocurrency payments: Few reputable businesses accept cryptocurrency as payment.

Seniors should learn to enable security features like two-factor authentication on payment apps and never share their login credentials or personal information.

Family members can support seniors by discussing these technologies, helping them verify suspicious messages and encouraging regular reviews of financial accounts.

Fighting Medical Scams

Scammers are increasingly targeting seniors with schemes designed to exploit Social Security and Medicare benefits.

© ADOBE STOCK

These essential programs provide critical support to older adults, making them prime targets for fraud. Recognizing the warning signs of these scams is vital to safeguarding personal information and financial security.

In 2023, there were reports of more than $126 million in losses, a 22.1% increase from the start of fiscal year 2023 to 2024. Those experiencing the greatest loss are seniors between the ages of 70 and 84.

SOCIAL SECURITY SCAMS: SPOT THE RED FLAGS

Fraudsters often pose as representatives of the Social Security Administration (SSA) to steal sensitive information. They may claim there is a problem with your Social Security number or benefits and insist you act immediately to avoid penalties.

Other fraudsters collect people's social security numbers to file false tax returns. Several years ago, the IRS uncovered $10 billion in tax fraud schemes.

The U.S. Department of Justice warns these fraudsters aren't just individuals, but, "large criminal enterprises with individuals at all stages of the scheme: those who steal the Social Security Numbers (SSN) and other personal identifying information, those who file false returns with the Internal Revenue Service (IRS), those who facilitate obtaining the refunds and the masterminds who promote the schemes."

Key warning signs of Social Security scams include:

• Receiving unsolicited calls or emails claiming to be from the SSA.

• Threats of arrest, legal action or suspension of benefits.

• Demands for immediate payment via gift cards, cryptocurrency or wire transfers.

• Requests for your Social Security number or banking information.

The SSA does not contact individuals by phone or email to demand personal information or payments. If you suspect fraud, hang up or delete the email. Verify any claims by contacting the SSA directly at (800)772-1213 or visiting ssa.gov.

MEDICARE FRAUD: PROTECTING YOUR BENEFITS

Medicare scams often involve fake representatives offering services or products in exchange for personal details. In some cases, fraudsters bill Medicare for unnecessary or nonexistent services, stealing from the program and jeopardizing your benefits.

COMMON MEDICARE SCAMS INCLUDE:

• Unsolicited calls or visits from individuals claiming to be Medicare representatives.

• Offers of "free" medical equipment, testing or services in exchange for your Medicare number.

• Pressure to sign up for additional plans or services you didn't request.

• Receiving bills for treatments or services you didn't receive.

To protect yourself, never share your Medicare number with anyone who contacts you unexpectedly. Review your Medicare Summary Notices (MSNs) regularly to ensure all claims are accurate. If you notice suspicious charges, report them to Medicare at (800) MEDICARE, (800) 633-4227.

TAKING ACTION AGAINST SCAMS

If you believe you've been targeted by a Social Security or Medicare scam, act promptly:

• Report Social Security scams to the Office of the Inspector General at oig.ssa.gov.

• Notify Medicare of suspected fraud at (800) MEDICARE or through the Medicare website.

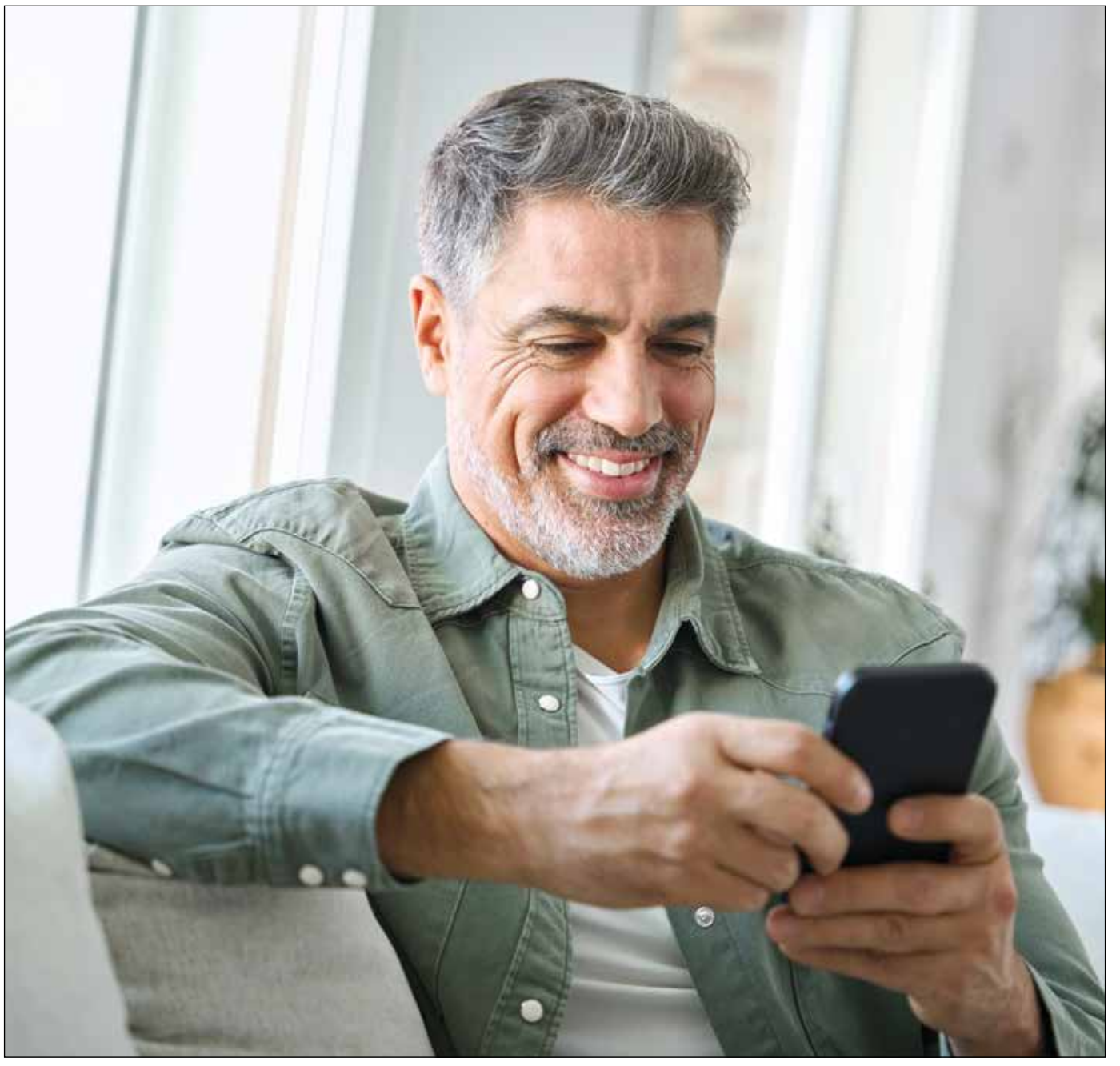
• Share your experience with trusted family members or local authorities to raise awareness.

The Senior Medicare Patrol (SMP) offers free assistance in identifying and reporting Medicare fraud. Visit smpresource.org to find a local program.

Social Security and Medicare scams can have devastating effects on seniors, but awareness is a powerful defense. By staying vigilant, recognizing red flags and reporting suspicious activity, seniors can protect themselves and these essential programs from exploitation.

Online Dating Schemes

Romance scams are a heartbreaking and costly form of fraud that prey on individuals seeking companionship, often targeting seniors who may feel isolated or lonely.



© ADOBE STOCK

These scams exploit emotional vulnerability, using trust and affection as tools to steal money or personal information.

According to the Federal Trade Commission (FTC), romance scams cost Americans nearly $1.14 billion in 2023, with seniors among the most affected groups. The median losses per person were $2,000.

HOW ROMANCE SCAMS WORK

Romance scammers typically operate on online dating platforms, social media or messaging apps. They create fake profiles using stolen photos and fabricated details, presenting themselves as attractive, caring and compatible individuals. Once they establish a connection, the scammers quickly work to build trust and emotional intimacy with their targets.

After gaining their victim's confidence, scammers often concoct urgent or tragic stories to request money. These might include claims of medical emergencies, travel expenses or sudden financial hardships. The FTC warns "sad stories are usually scam stories." Payments are usually requested through untraceable methods such as wire transfers, prepaid cards or cryptocurrency.

In some cases, scammers ask for personal information under the guise of strengthening the relationship, which can later be used for identity theft.

WHY SENIORS ARE TARGETED

Seniors are particularly vulnerable to romance scams for several reasons:

- **Loneliness:** Older adults, especially those who are widowed or living alone, may turn to online platforms for companionship.
- **Financial stability:** Seniors often have savings or fixed incomes, making them appealing to scammers.
- **Lack of digital familiarity:** Seniors may be less experienced with online scams and less likely to recognize red flags.

RECOGNIZING THE WARNING SIGNS

Educating seniors about the common characteristics of romance scams can help protect them:

- **Fast-tracked relationships:** Scammers often express intense feelings or push for exclusivity early in the conversation.
- **Avoiding in-person meetings:** Scammers consistently have excuses for not meeting face-to-face, claiming to be in the military, working overseas or dealing with personal challenges. Those type of excuses are red flags the person giving them is a scammer.
- **Requests for money:** Any request for financial assistance, especially from someone you've never met in person, is a major red flag.
- **Inconsistent stories:** Discrepancies in their personal narrative, photos or online presence can be indicators of a scam.

HOW TO STAY SAFE

Seniors can protect themselves by following these steps:

- **Verify identities.** Use reverse image searches or online tools to check if a profile photo appears elsewhere.
- **Keep money off the table.** Never send money or gifts to someone you haven't met in person.
- **Involve others.** Discuss online relationships with family or trusted friends who may spot warning signs. Romance scammers will insist the relationship be kept a secret.
- **Report suspicious activity.** Notify the platform where the scam occurred and file a report with the FTC or FBI's Internet Crime Complaint Center (IC3).

Fraudulent Travel Offers

Travel is a cherished activity for many seniors, offering opportunities for relaxation, exploration and connection with loved ones.

© ADOBE STOCK

Unfortunately, scammers often target older adults with fraudulent vacation deals and timeshare offers that promise incredible value but deliver nothing but financial loss and frustration.

HOW TRAVEL SCAMS WORK

Travel scams come in many forms, from fake vacation packages and counterfeit airline tickets to high-pressure timeshare sales and fraudulent rental properties. Scammers advertise alluring deals through emails, social media or online ads, often requiring upfront payments to secure the offer. Once the payment is made, the scammer disappears, leaving the victim without a trip or recourse.

Timeshare scams are another common tactic. Fraudsters may convince seniors to buy into nonexistent timeshares or charge fees for services like reselling a timeshare that never materialize. They exploit the desire for affordable vacation options while trapping victims in costly agreements.

WHY SENIORS ARE VULNERABLE

Seniors are appealing targets for travel scams because they:

• **Seek relaxation or adventure.** Retirement often provides time to travel, making seniors more likely to respond to enticing offers.

• **Value affordability.** Fixed incomes may prompt seniors to jump at deals promising significant savings.

• **Trust easily.** A lifetime of experience can sometimes make seniors overconfident in their ability to detect fraud.

COMMON WARNING SIGNS OF TRAVEL SCAMS

• Unbelievable deals: Offers that seem too good to be true, such as deeply discounted cruises or free accommodations, are often scams.

• Pressure to act quickly: Scammers create urgency, insisting that deals must be booked immediately to secure the price.

• Vague details: Legitimate companies provide clear terms, conditions and contact information. Scammers often avoid specifics or fail to provide written documentation.

• Upfront payments: Requests for full payment via wire transfer, gift cards or cryptocurrency are significant red flags.

HOW SENIORS CAN STAY SAFE

• **Research thoroughly.** Verify the legitimacy of travel companies by checking online reviews, Better Business Bureau ratings and official websites.

• **Avoid unsolicited offers.** Be cautious of unsolicited emails, calls or ads offering travel deals.

• **Read the fine print.** Carefully review the terms and conditions of any travel package or timeshare agreement.

• **Pay securely.** Use credit cards for transactions, as they often provide fraud protection.

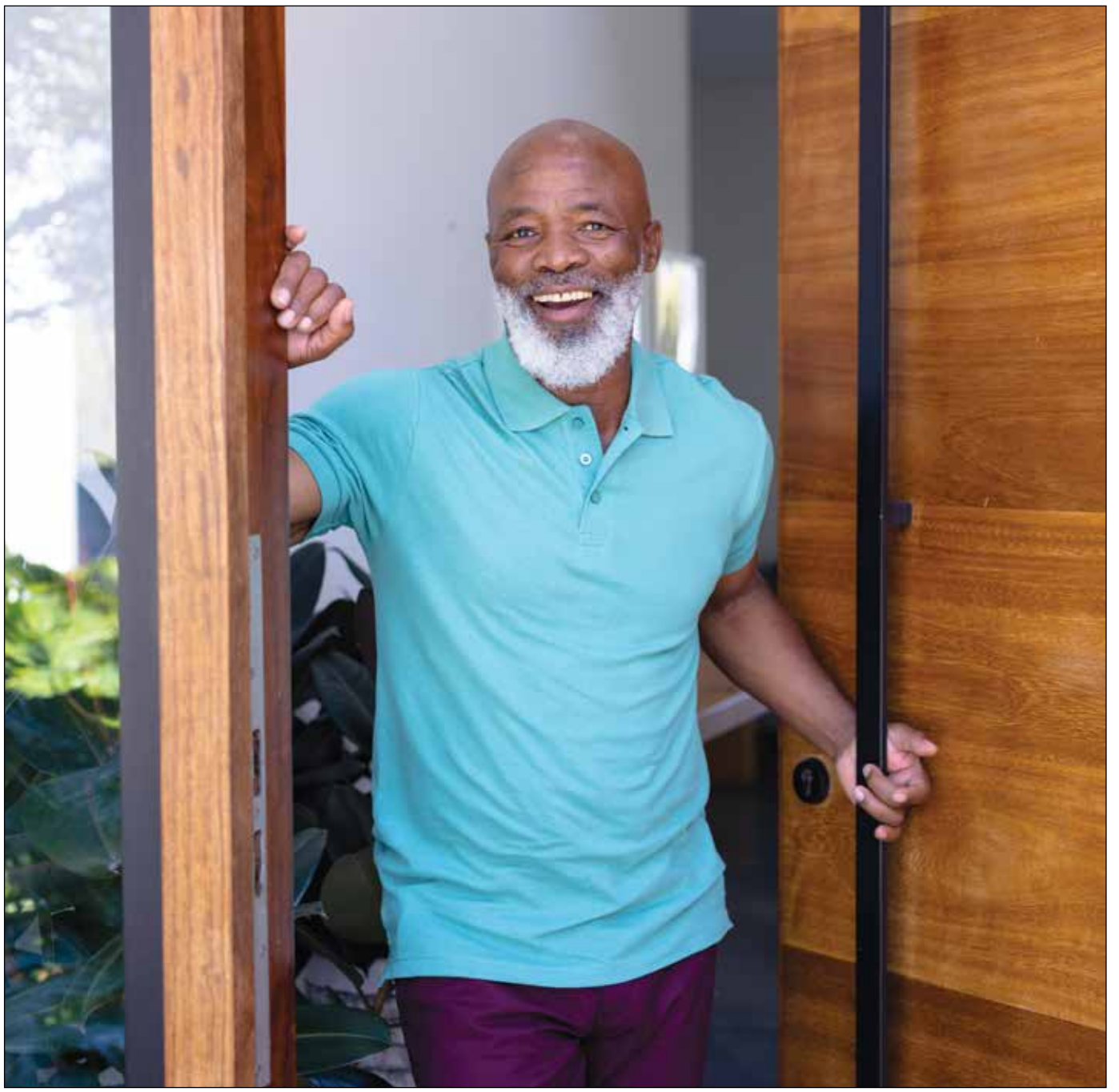
• **Seek professional advice.** Consult a trusted travel agent or legal expert before signing any contracts.

RESOURCES FOR ASSISTANCE

Seniors who suspect they've fallen victim to a travel scam should report it to the Federal Trade Commission (FTC) or their state's consumer protection agency. The AARP Fraud Watch Network also provides information and support for seniors dealing with scams.

Look Out for Utility Scams

Utility scams are a common tactic used by fraudsters to exploit seniors, often preying on their fear of losing essential services like electricity, water or gas.



© ADOBE STOCK

These scams usually involve fraudulent calls or emails demanding immediate payment for supposed overdue bills, accompanied by threats to cut off service.

According to the Federal Trade Commission (FTC), scams related to utilities are on the rise, costing Americans millions each year. Seniors, who may be less familiar with modern fraud tactics, are particularly vulnerable.

HOW UTILITY SCAMS OPERATE

Scammers often impersonate representatives from trusted utility companies, using caller ID spoofing to make their communication appear legitimate. They claim the senior's account is overdue and demand immediate payment to avoid service disruption. Payment is typically requested via untraceable methods such as prepaid debit cards, gift cards or wire transfers.

In some cases, fraudsters may send emails resembling official utility company correspondence. These emails often include logos and branding to appear authentic, with links leading to fraudulent websites designed to steal personal or financial information.

WHY SENIORS ARE TARGETED

Seniors are frequently targeted because they are more likely to have steady incomes or savings and may be less familiar with digital payment systems or cybersecurity measures. Additionally, many seniors live alone, making them more susceptible to high-pressure tactics, especially when threatened with immediate consequences like a utility shut-off.

RECOGNIZING UTILITY SCAMS

Educating seniors to recognize common red flags is essential to preventing these scams:

- **Unsolicited contact:** Utility companies rarely make unexpected calls or send emails demanding payment. Legitimate notifications are typically mailed or sent through established account portals.
- **High-pressure tactics:** Scammers create urgency by threatening immediate disconnection, which utility companies generally do not do without prior notice.
- **Unusual payment methods:** Requests for payment via gift cards, wire transfers or prepaid cards are almost always scams.
- **Errors in correspondence:** Emails from scammers often include spelling errors, generic greetings or links to unofficial websites.

WHAT TO DO IF CONTACTED

If seniors receive a suspicious call or email, they should:

- **Hang up or delete.** Do not engage or click on links.
- **Verify with the utility company.** Use the contact information listed on a recent bill or the company's official website.
- **Report the incident.** Notify local law enforcement or consumer protection agencies like the FTC or the Better Business Bureau.

HOW TO STAY SAFE

Seniors can protect themselves by enrolling in online account management with their utility providers, enabling them to track their bills and payments directly. Additionally, families and caregivers should encourage seniors to use call-blocking technologies and be cautious about sharing personal information over the phone or email.

By staying informed and vigilant, seniors can avoid falling victim to these scams, ensuring their peace of mind and financial security remain intact.