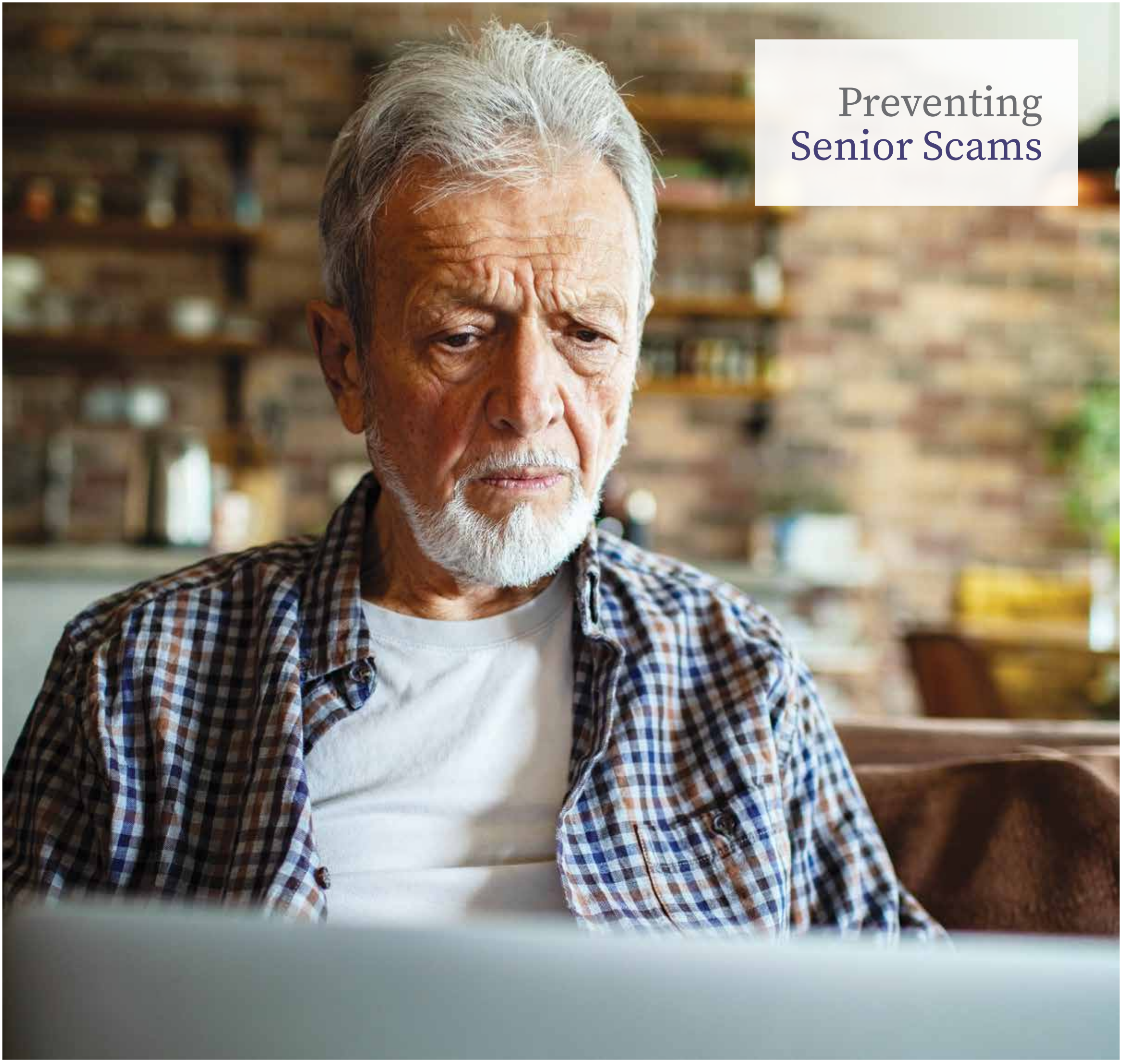
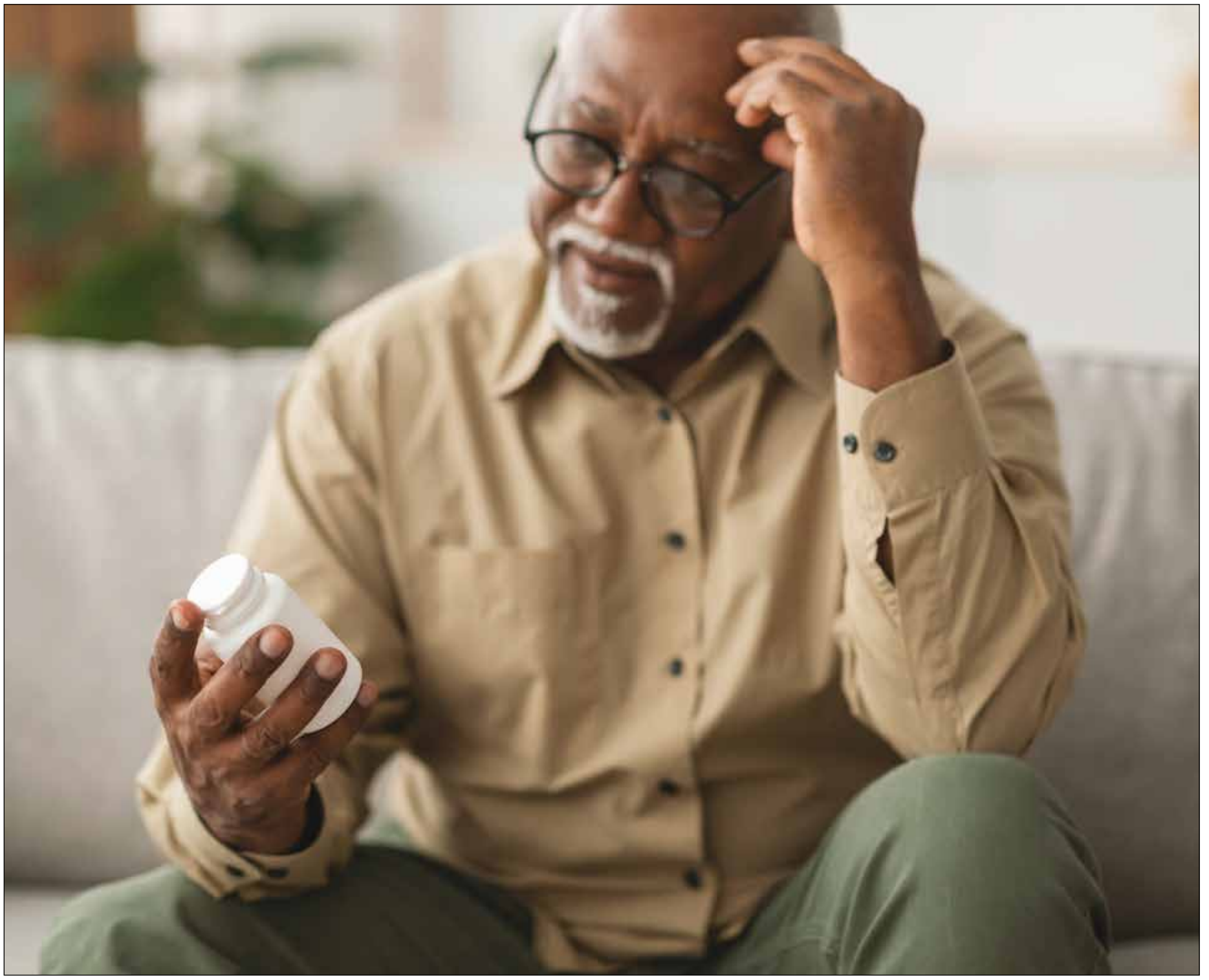
Preventing Senior Scams



© ADOBE STOCK

The Most Common Scams

Older adults are especially at risk for several types of scams, the most common of which are healthcare fraud, fake prescription drugs and funeral scams.



© ADOBE STOCK

Here are some tips on how to prevent yourself from becoming a victim.

HEALTHCARE FRAUD

Those aged 65 and over are particularly vulnerable to healthcare fraud because all American seniors qualify for Medicare. Information about this government-sponsored health program is accessible to the public, making it easy for someone to impersonate a knowledgeable Medicare "representative" either through phone calls or online communications. They may not be legitimate. Always be cautious with anyone who requests personal details. Ask for their name and official identification, then disconnect and call the agency directly to verify their identity.

FUNERAL SCAMS

There has been a sharp uptick lately in funeral scams. One popular scheme promotes pricier caskets or funeral packages. Fraudsters may falsely claim that such expenses are legally mandated. This, of course, is inaccurate. Some have even used publicly available obituaries to target mourners at funeral services for people the criminal never knew. Officials have reported that more seniors are being contacted in an attempt to collect non-existent debts.

COUNTERFEIT PRESCRIPTIONS

Many seniors attempt to manage their retirement budgets by cutting back on routine expenses.

One way to save money is by cutting the cost of medications. But false or misleading ads make older Americans an easy target for the increasing number of online drug scams. Seniors may be at risk of losing both their hard-earned savings and good health, since these drugs are still expensive and often fake. If you aren't currently using a reliable website to order medications, ask your doctor, friends or family members for recommendations on safe online alternatives.

Filing a Report

Have you or an older loved one been the victim of fraud?

© ADOBE STOCK

Scams aimed at older adults are increasing, as con artists employ more advanced techniques to steal money or personal details. It's important to understand what to do next.

Promptly notifying authorities will increase the likelihood of recovering stolen funds. If you or an older loved one falls victim to one of these schemes, it's only natural to have feelings of embarrassment – but don't let that stop you from reporting the incident. Here's how:

IDENTIFY THE SCAM

Before making a report, confirm that you have indeed fallen victim to a scam. Common indicators include an unexpected communication requesting money or personal information. They may create deadline pressure to take action to avoid negative consequences. Others may demand payment through untraceable means like wire transfers, cryptocurrency or gift cards. Finally, note any offers of rewards or services that seem too good to be true.

COLLECTING INFORMATION

When reporting a scam, gathering the most information will make your report more useful to investigators. Try to collect any names that the scammer uses, as well as phone numbers, email addresses or websites associated with the scammer. Note anything the con artist promised. Keep copies of emails, letters or text messages that you received, along with details about transactions like amounts, dates and payment methods.

WHO TO CONTACT

Your specific kind of scam determines which agency needs to be contacted. If you're unsure, call the National Elder Fraud Hotline at (833) 372-8311. This is a free service established that assigns case managers to callers to assist seniors throughout the reporting process.

Those who have lost money or personal property should file a report with their local police department. Scams involving businesses within your state should be reported to your state attorney general's office. Ask for the consumer protection division. Victims of online shopping fraud, phishing and imposter scams should contact the Federal Trade Commission at ReportFraud.ftc.gov. Report online scams and cybercrimes to the FBI's Internet Crime Complaint Center at ic3.gov.

If you need more general support and complimentary resources, call AARP's Fraud Watch Network helpline at 877-908-3360. Members of your community may be able to offer assistance.

What to Watch For

Cybercrime has been around for a while, but the fraudster's approaches are constantly changing.

© ADOBE STOCK

Their advanced new techniques are also targeting different areas of our lives. Here's what to watch out for:

ROBOCALLS

Scammers using new computer technology can make automated calls to reach seniors from any global location. Some of these so-called "robocalls" may claim that an insurance policy or warranty on a vehicle needs immediate renewal. Another increasingly prevalent scam involves asking the recipient, "Can you hear me? " Once a senior answers in the affirmative, their voice is recorded and the call ends. This recorded response can then be used to authorize charges on stolen credit cards.

SWEEPSTAKES AND LOTTERY

Con artists will claim that a senior has won a lottery or some sort of prize, but they need to send cash or gift cards to cover imaginary taxes or processing fees to get access to the winnings. They may falsely present themselves as representatives from contest organizations like Publishers Clearing House to gain a victim's trust. Ultimately, no prize is awarded and a senior ends up losing money.

GOVERNMENT IMPERSONATION

In these schemes, scammers pose as representatives from government agencies like Social Security, the IRS or Medicare. Their goal is to extract personal information after lying about things like overdue taxes. The info you share is then exploited for identity theft. Imposters may insist on using payment methods that are hard to track, like cash, prepaid debit cards or wire transfers.

TECH SUPPORT

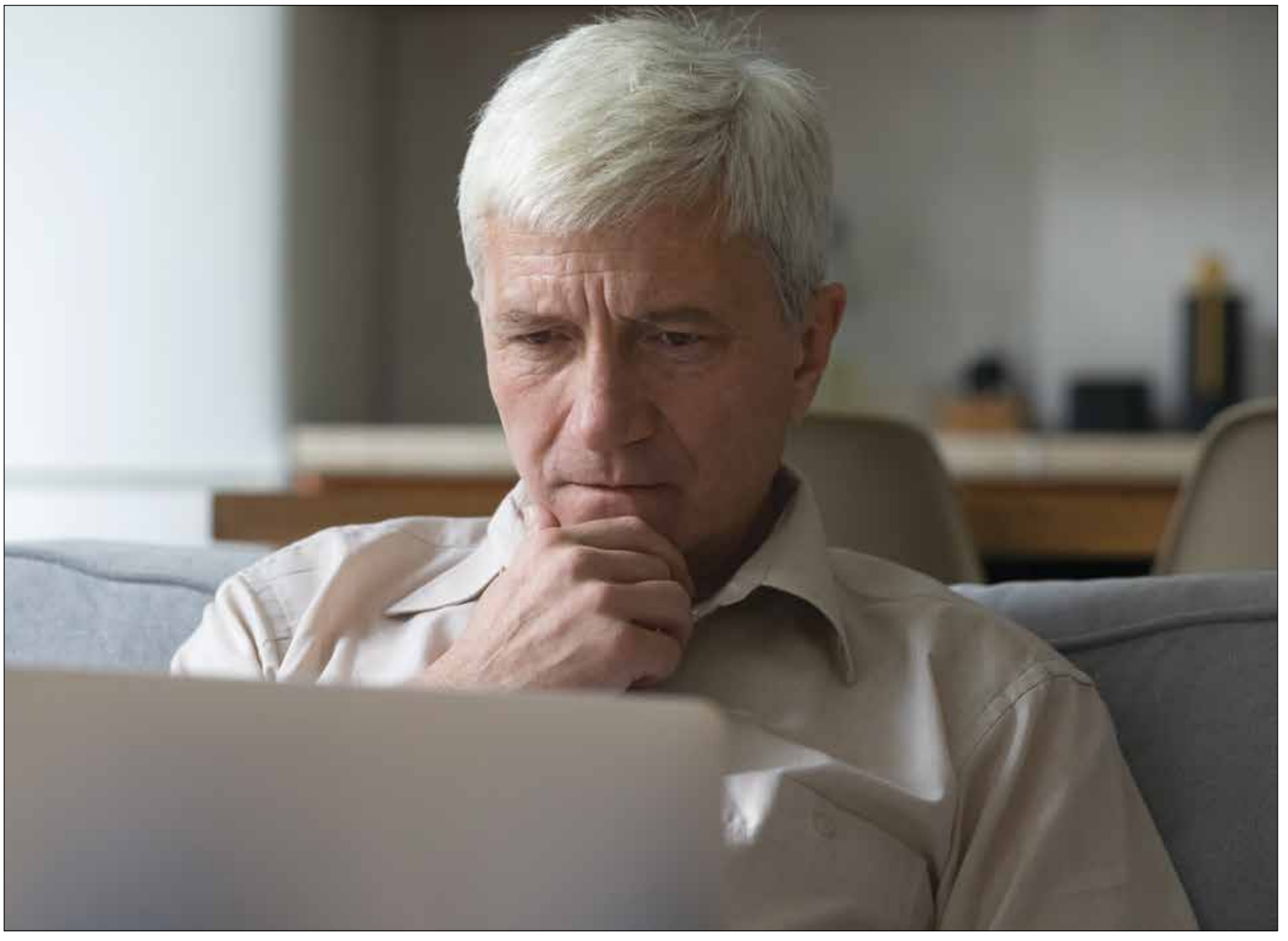
Others are taking aim at seniors by triggering a pop-up message or displaying a blank screen on phones and computers, both of which seem to indicate that the device requires some sort of repair. When the victim calls a provided support number, the scammer then asks for remote access or demands payment for repair services.

BAIT AND SWITCH

In this scam, a fraudster poses as a grandchild and asks seniors to guess their identity. If the grandparent mentions someone by name, the scammer then claims the grandchild needs money to resolve some kind of urgent situation like bail or car repairs. The scammer might also pose as a police officer, lawyer or doctor who is offering assistance, only to then ask for money.

Combatting E-Mail Scams

Email has made it easier than ever to stay in touch with friends, family and consumer contacts. But its ease of use also opens the door to what's known as "phishing" scams.



© ADOBE STOCK

Phishing is a form of cybercrime where the attacker attempts to obtain sensitive data such as user names, credit card information, passwords or other personal details by masquerading as a trustworthy source.

Seniors often have a heightened vulnerability to these misleading emails, because of their unfamiliarity with the elements of these scams. The scheme often begins with statements like "your bank account has been compromised" or "you're the grand prize winner." Phishing typically occurs through email, but can also happen through instant messaging, social media or phone calls.

IDENTIFYING THREATS

Identifying phishing emails involves careful scrutiny of the sender's email address. Fraudulent actors frequently use misleading addresses that might seem authentic at first glance. Look for any peculiarities or spelling mistakes in the sender's email domain. The messages themselves might feature grammatical or spelling mistakes. Be extremely cautious if you see awkward sentence constructions. Reputable organizations usually have a higher standard.

Prevent yourself from falling victim to phishing by verifying all attachments and links. Scammers often try to create a sense of urgency or fear to encourage email recipients to act quickly.

Avoid clicking on unexpected links or opening attachments. Authentic emails typically share important updates through secure channels.

Be cautious with emails that encourage hasty decisions or pressure you into sharing sensitive information.

HOW TO PROTECT YOURSELF

Activate two-factor authentication whenever possible. This security measure requires a second verification method, like a code sent to your mobile phone, before access is granted. Never share personal information via email, nor verify sensitive data like bank account numbers, addresses and phone numbers, or Social Security numbers. Avoid sharing personal details over the phone, especially if the caller reached out to you. Instead of clicking on website links, manually enter the site's web address. Keep your devices and security software updated; regular updates often include fixes that guard against the latest phishing strategies.

Keeping Medical Info Safe

Fraudsters can use data from the healthcare system to wreak havoc.

© ADOBE STOCK

Health care fraud can manifest in many ways, from misleading billing methods to outright identity theft. Since seniors frequently depend on health care services, they're particularly vulnerable to con artists who attempt to take advantage of their trust. Identifying the warning signs is essential for protecting both personal safety and financial health.

MEDICARE CONCERNS

Unfortunately, more seniors are falling victim to Medicare fraud. Typical examples of these scams involve billing for services or products that were never received, misusing a Medicare number for false claims, charging twice for the same service, and providing unauthorized Medicare drug plans. To help limit your exposure to health care fraud, keep your Medicare cards secure, always be skeptical of unsolicited offers for free medical services or equipment, and be careful about sharing your Medicare information.

DOCTORS AND INSURANCE

Before getting any kind of medical care, verify the qualifications of health care providers and the facility to make sure they are licensed and accredited. You don't want to pay for substandard care. Be wary of salespeople who come to the door to sell healthcare services or products, as well. Exercise caution when presented with so-called "free" screenings or services, and confirm the identity of anyone claiming to represent your insurance company, Medicaid or Medicare. Routinely check your explanation of benefits statements for any unfamiliar charges or services – and immediately ask questions about any unusual entries.

STAY AWARE

Secure all your online medical accounts with distinct, hard-to-guess passwords. Keep all of the security software on computers, smartphones and tablets updated, since that's your first line of defense against online con artists. To protect personal and medical data, shred any medical documents that contain sensitive information before you dispose of them.

Stay educated about common health care scams. Being aware of the tactics used by scammers helps seniors spot potential risks and avoid being deceived by the latest schemes. If you suspect health care fraud, report it immediately to Medicare at (800) MEDICARE or to the fraud hotline of your insurance provider. This enables the authorities to act quickly.

Avoiding Housing Schemes

Everyone wants safe, secure housing, and con artists will take advantage.

© ADOBE STOCK

Common housing scams focus on seniors who are owners of family homes that are fully paid off or who might need to alter their living arrangements due to health concerns. This can make them susceptible to reverse mortgage fraud. Scammers use a range of strategies, including fake property listings, bogus property management schemes and non-existent rentals to mislead their victims. Here's how to avoid these fraudulent schemes.

BEFORE YOU BEGIN

Before entering into any rental agreement, thoroughly check property listings. Consult trustworthy real estate websites, while exercising caution with advertisements that show overly attractive options or lack critical information. Whenever possible, visit the property in person prior to making any financial decisions. Scammers typically avoid face-to-face meetings and may make up excuses to defer visits. Some rental listings may promise unrealistically low prices for properties in high demand, as these enticing offers are often used to bait victims into sharing personal and financial details.

DO YOUR RESEARCH

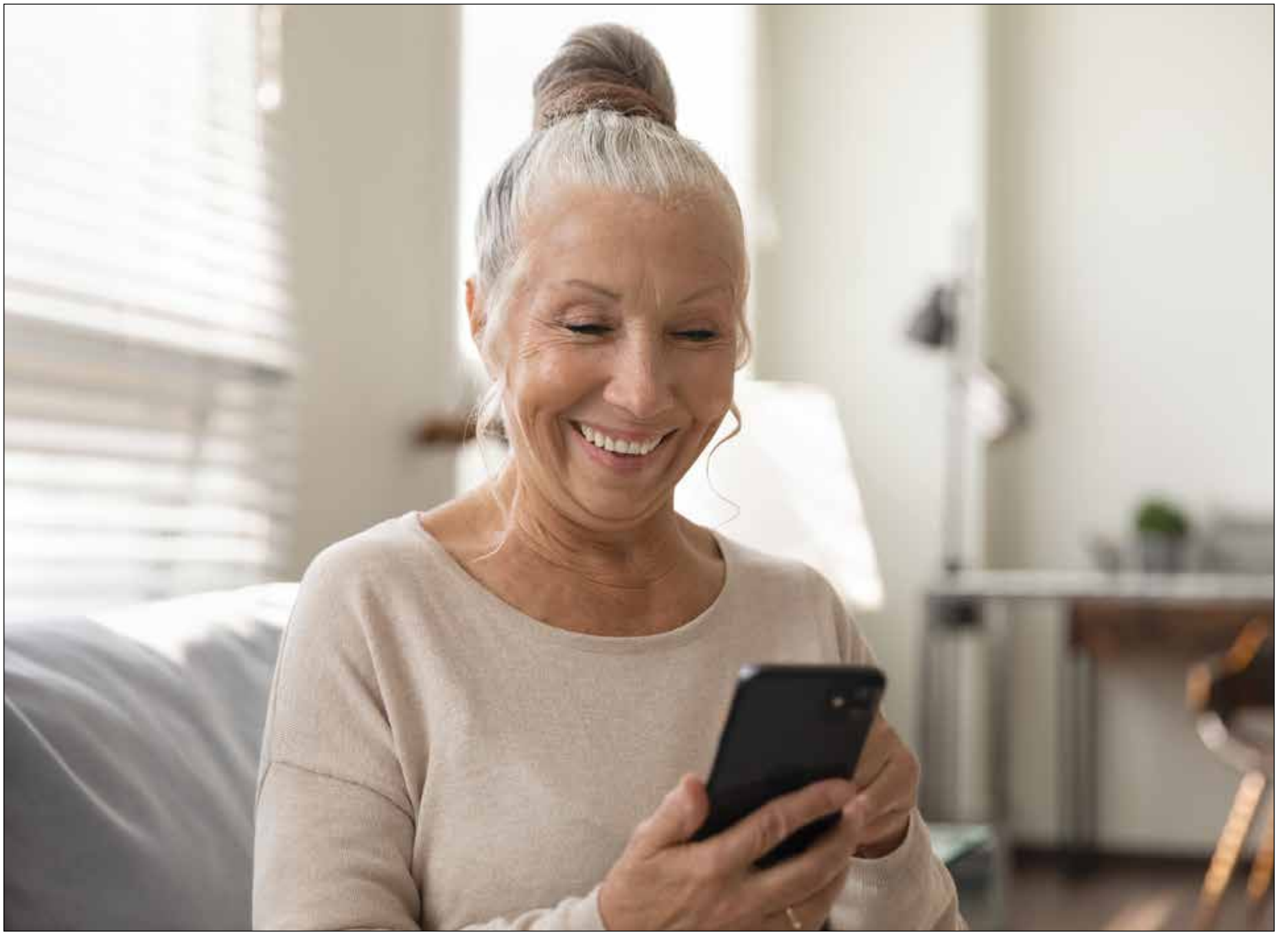
Reverse mortgages are available to homeowners age 62 and above as a means of accessing built-up home equity. The concept itself is not inherently deceptive, but some individuals target seniors with fake reverse mortgages. They may offer help in gaining access to their equity, only to embezzle the funds or commit deed fraud to take control of the home. Other schemes include false promises of quick approval for a reverse mortgage to prevent foreclosure – in exchange for an illegal fee. Unscrupulous contractors who visit seniors may offer free consultations to persuade homeowners to secure reverse mortgages for unnecessary upgrades or home repairs.

ADDITIONAL ADVICE

Prior to entering into any reverse mortgage agreement, confirm the lender's credentials. Ensure they are trustworthy and licensed. If you're unfamiliar with the terms and conditions of the mortgage, get independent counsel from financial advisors so you can fully grasp the associated risks and advantages. Scammers might employ high-pressure tactics to rush seniors into quick decisions. Don't let anyone push you into hastily signing documents. Always bank with established and reliable financial institutions, longstanding government agencies and recognized financial advisors. When making rent payments or deposits, only use secure and traceable methods. Steer clear of cash transactions or wire transfers, since they provide minimal recourse in cases of fraud.

Safer Online Dating

Romance scams can be devastating for seniors, both emotionally and financially.



© ADOBE STOCK

Seniors who experience feelings of isolation or loneliness are especially vulnerable to dishonest online dating schemes. Con artists try to build the appearance of trust and affection to steal sensitive personal data or financial resources. The scams are resulting in more than $1 billion in losses per year, with older Americans being among the most affected. Experts say the average loss is $2,000. Here's how to keep yourself, your friends or your family members safe:

HOW THEY WORK

Romance scammers will typically engage with victims through online dating sites, messaging applications or social media. They create deceptive profiles, using stolen images and false information, then present themselves as attractive, compatible and caring potential partners. Once a connection is made, they begin to focus on creating a sense of emotional closeness with their victims. Once they've won the target's confidence, scammers then tend to develop urgent or tragic narratives while soliciting financial help.

These urgent situations may include a big medical bill or other unexpected financial difficulties. Payments are frequently requested through untraceable channels, such as wire transfers, cryptocurrencies or prepaid cards. Scammers may seek personal information under the pretense of growing the relationship, then later use the details for identity theft.

WARNING SIGNS

Seniors tend to be particularly susceptible to romance scams due to loneliness. Many older people may seek companionship online, particularly those who have lost a spouse or live alone. Many seniors have a large amount of savings or pension income. Finally, they might have limited digital experience, making them too unfamiliar with online scams to identify the warning signs.

Scammers often display overwhelming emotions or an urge to become exclusive too early in the interaction. They always have reasons for not meeting face-to-face. Any solicitation for money is a serious warning sign, particularly from those who seniors only know online.

KEEPING SAFE

Do not send money or gifts to anyone you have not met face-to-face. Talk about online relationships with family members or reliable friends who can help identify potential warning signs.

Finally, report any suspicious behavior. Inform the social media platform operator and submit a report to the FTC or the FBI's Internet Crime Complaint Center.