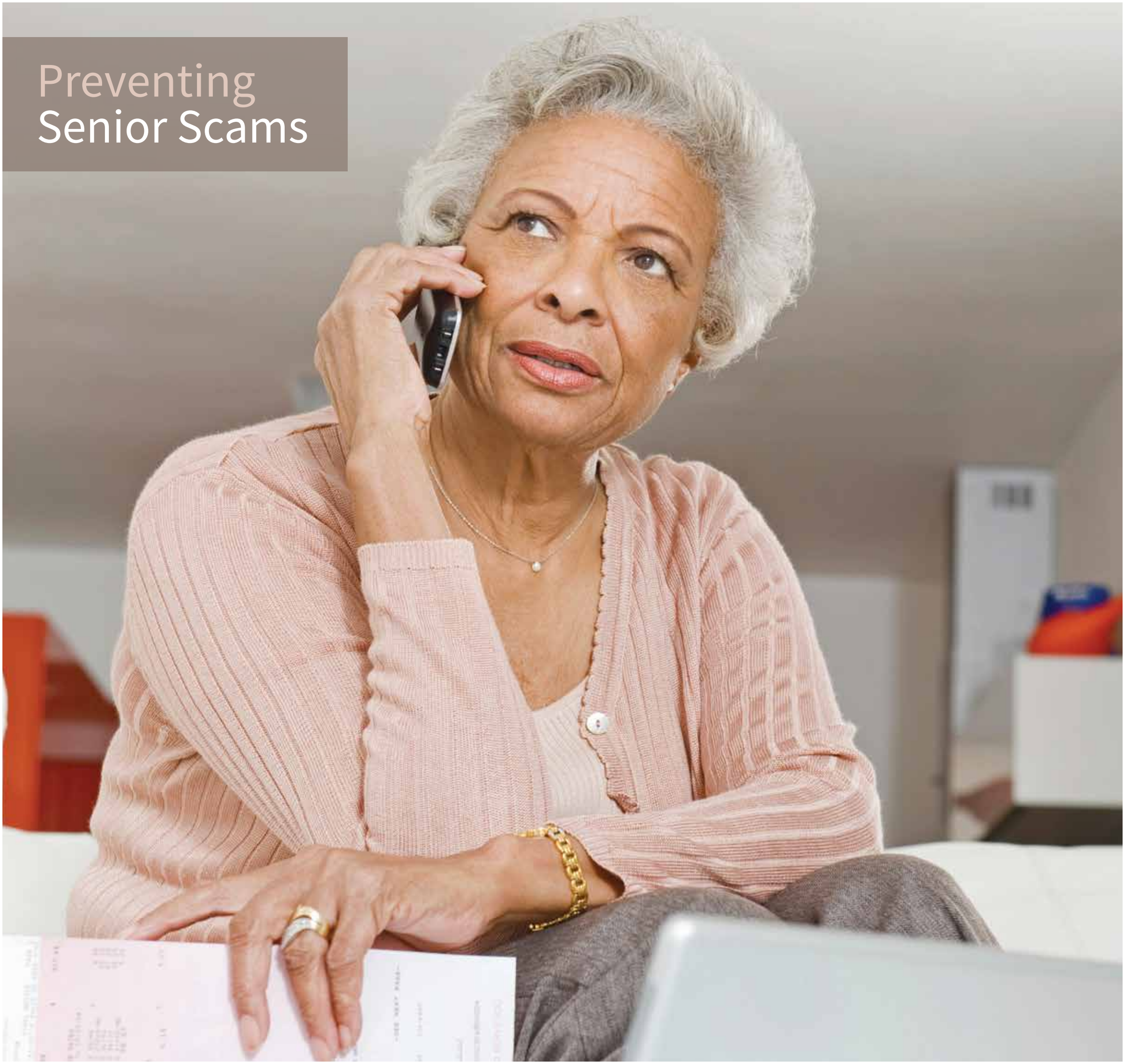
Preventing Senior Scams



© ADOBE STOCK

Dodge Online Shopping Scams

Online shopping has become a convenient way for seniors to access a myriad of products. However, with the convenience comes the need for vigilance.

© ADOBE STOCK

According to the FBI, online shopping scams were the second most reported fraud among seniors in 2021 — they received more than 13,000 complaints of fraudulent products and non-delivery.

The online shopping landscape is vast, offering a multitude of choices at the click of a button. Unfortunately, it also opens the door to potential scams and fraudulent activities. Understanding the risks is the first step towards safer online shopping.

Stick to well-known and reputable online retailers. Recognizable names often have established security measures to protect customer information. If in doubt, research customer reviews and ratings to gauge the reliability of the website.

Ensure the website is secure by looking for "https://" in the URL and a padlock icon in the address bar. This indicates that the website encrypts data during transmission, protecting your personal and financial information.

Regularly update your device's software and install reliable antivirus programs. This helps safeguard against potential security vulnerabilities and protects your system from malicious software.

Create strong, unique passwords for each online shopping account. A combination of letters, numbers and special characters enhances security. Avoid using easily guessable information, such as birthdays or names.

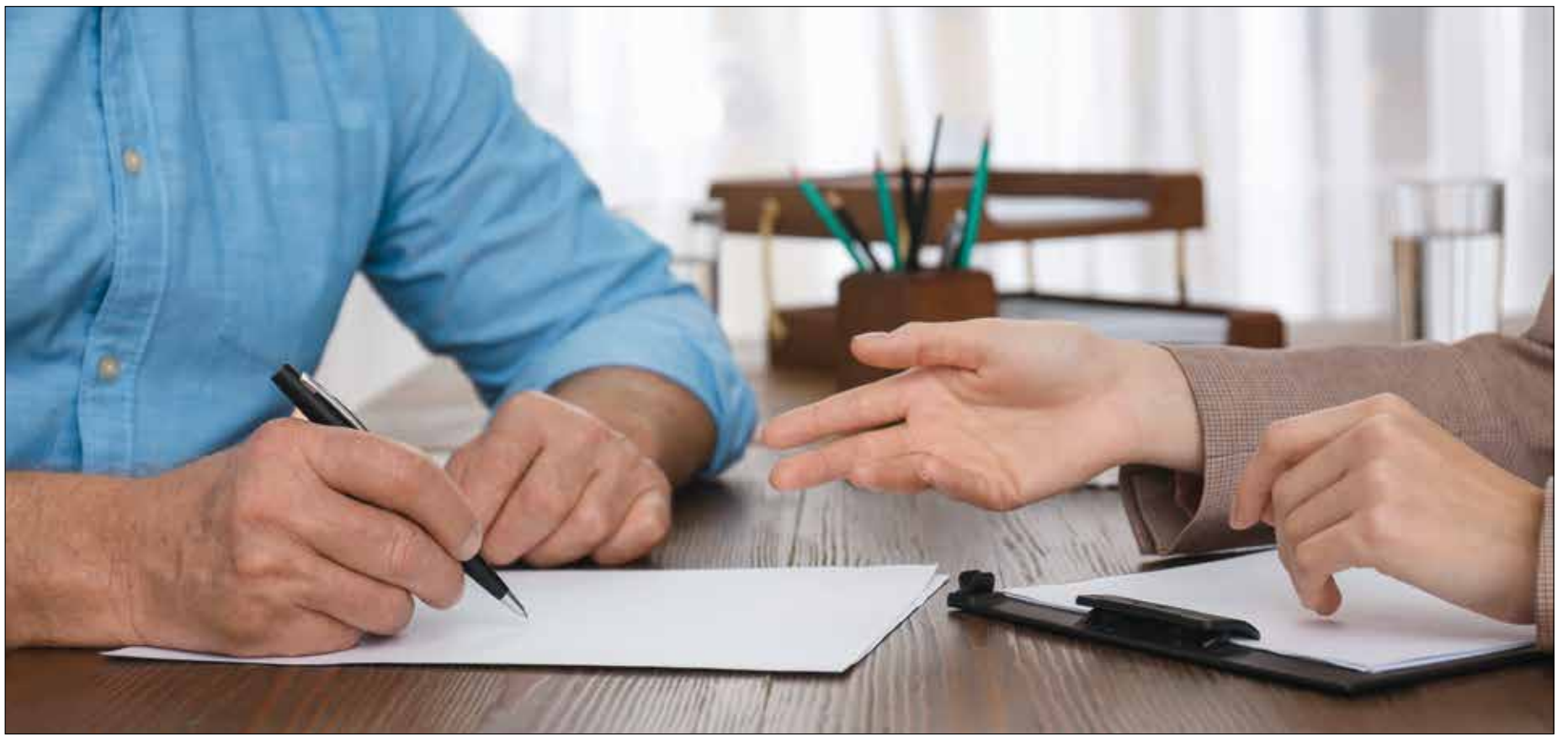
Be cautious of unsolicited emails or messages claiming to be from online retailers. Legitimate companies rarely ask for sensitive information through email. Verify the authenticity of such communications independently before taking any action. Familiarize yourself with the privacy policies of online retailers. Reputable websites are transparent about how they handle your data. Avoid websites that lack clear privacy policies or seem reluctant to share this information.

Opt for secure payment methods, such as credit cards or trusted online payment services. These methods offer additional layers of protection, and credit cards often provide the option to dispute charges in case of fraudulent activity. Legitimate online retailers provide clear contact information, including a physical address and customer support details. If a website lacks this information or provides only an email address, exercise caution.

Regularly review your bank and credit card statements for any unauthorized transactions. Report any discrepancies to your financial institution immediately to prevent further unauthorized access. Stay informed about common online scams. Understanding the tactics used by cybercriminals can help you recognize potential threats and avoid falling victim to deceptive practices.

Unmasking Financial Scams

Investors must remain vigilant against the rising tide of investment scams that aim to swindle hard-earned money. Seniors in particular are often targets of investment fraud, particularly Ponzi schemes.



© ADOBE STOCK

Investment scams come in various forms, with perpetrators often employing enticing promises of high returns with minimal risk.

According to Aura, a security firm, the most common types of investment frauds targeting seniors are:

Ponzi schemes: a notorious type of investment fraud that claims that there are high returns with little to no risk, but it generates money from new investors rather than earning any actual returns or profit.

Illegitimate bonds and certificates of deposit (CDs): Fraudsters entice seniors into investing in low-risk bonds or CDs that don't actually exist or do not give the return that the sellers claim.

Charitable gift annuities: These scams claim that if a donor gives a large sum of money as a donation, they'll get a fixed income stream for as long as they live. However, these charities often don't exist and the income stream never shows up.

Prime bank scams: Fraudsters claim to have access to secret markets overseas that allow for large returns. However, there are no such markets and any money given to the con artist disappears into their pocket.

RED FLAGS

Be wary of investment opportunities promising guaranteed high returns with little or no risk. Legitimate investments always carry a degree of risk, and promises that sound too good to be true often are. Scammers frequently use high-pressure tactics to prompt quick investment decisions. If you feel rushed or pressured to invest without adequate information, step back and reassess the situation.

Legitimate investment opportunities provide clear and transparent information about their offerings. Be cautious if the details of the investment are unclear or if the promoter avoids providing comprehensive information. Verify the credentials of individuals or firms offering investment opportunities. Legitimate financial professionals are registered with relevant regulatory authorities. Check the credentials of those promoting investment opportunities before committing any funds.

AVOIDING INVESTMENT SCAMS

Before investing, thoroughly research the investment opportunity, the individuals involved, and the company promoting the investment. Verify the legitimacy of the investment by checking with regulatory bodies and seeking independent reviews.

Diversification is a key strategy in mitigating risk. Avoid putting all your funds into a single investment, as this can expose you to higher risks. Diversifying across different asset classes helps safeguard your portfolio.

Consult with a licensed financial advisor before making investment decisions. A reputable advisor can provide valuable insights, assess risks and guide you toward legitimate investment opportunities aligned with your financial goals.

Exercise caution if you receive unsolicited investment offers through cold calls, emails or social media. Scammers often use these channels to target unsuspecting individuals. Verify the legitimacy of any unsolicited offers independently.

Keep yourself informed about common investment scams and fraud trends. Knowledge is a powerful defense against financial fraud. Regularly update yourself on potential risks in the investment landscape. A basic understanding of investing principles can empower you to make informed decisions. Familiarize yourself with common investment terms, risks and strategies to navigate the complex world of finance.

© ADOBE STOCK

Safeguard Medical Info

Seniors must navigate the health care landscape with vigilance to protect themselves from potential scams.

Health care fraud comes in various forms, ranging from deceptive billing practices to identity theft. Seniors, often reliant on health care services, are prime targets for scammers seeking to exploit their trust. Recognizing the red flags helps safeguard personal well-being and financial security.

Medicare.gov gives the following examples of common forms of Medicare fraud:

• A senior is charged for services or supplies that they never received.

• A provider charges twice for a service that a senior received only once or an item they received only once.

• Someone steals a Medicare number or card and uses it to submit fraudulent claims.

• A company offers a Medicare drug plan that Medicare hasn't approved.

TIPS FOR RECOGNIZING HEALTH CARE FRAUD

Safeguard your Medicare card as you would your credit cards. Avoid sharing your Medicare number unless necessary for trusted health care services. Be cautious of unsolicited calls, emails, or messages offering free medical services or equipment. Legitimate health care providers and insurance companies do not typically initiate contact in this manner.

Before seeking medical services, verify the credentials of health care providers. Ensure they are licensed professionals or recognized institutions. Scammers may pose as healthcare professionals to exploit vulnerable individuals.

Regularly review your explanation of benefits statements from Medicare or your insurance provider. Look for any unfamiliar services or charges, and report discrepancies immediately.

Be cautious of door-to-door salespeople offering health care services or products. Legitimate health care providers typically do not engage in unsolicited house calls. Exercise caution when offered "free" services or screenings. Scammers may use this guise to collect personal information for identity theft or fraudulent billing.

When receiving calls from individuals claiming to represent Medicare or insurance companies, verify their identity. Legitimate entities will provide clear information and will not press for immediate decisions.

SAFEGUARDING INFORMATION

Shred documents containing personal or medical information before disposing of them. This prevents sensitive information from falling into the wrong hands. Protect online medical accounts with strong, unique passwords. Avoid using easily guessable information and consider using a combination of letters, numbers and special characters.

Ensure your computer, tablet and smartphone have up-to-date security software. Regularly update operating systems and applications to address potential vulnerabilities. Stay informed about common health care scams. Understanding the tactics employed by scammers empowers you to recognize potential threats and avoid falling victim to fraudulent practices.

If you suspect health care fraud, report it promptly. Contact Medicare at (800) MEDICARE or your insurance provider's fraud hotline. Reporting helps authorities take swift action against scammers.

Recognizing Housing Scams

Everyone needs safe and secure housing, a fact that con artists will take advantage of to swindle people out of their money.

© ADOBE STOCK

Some of the schemes specifically target seniors who may have to change housing situations because of medical issues or have paid-off family homes making them vulnerable to reverse mortgage scams.

Rental and housing scams often exploit the vulnerability of those seeking safe and suitable living arrangements, and seniors can be particularly susceptible. Fraudulent listings, phantom rentals and fake property management schemes are some of the tactics employed by scammers to deceive unsuspecting individuals. Recognizing these scams is the first step in securing safe housing arrangements.

TIPS TO AVOID RENTAL AND HOUSING SCAMS

Before committing to any rental arrangement, thoroughly verify property listings. Use reputable real estate websites, and be cautious of listings that seem too good to be true or lack essential details.

Whenever possible, physically visit the property before making any financial commitments. Scammers often avoid in-person meetings and may provide excuses to discourage property visits. Be skeptical of rental listings that offer exceptionally low prices for high-demand properties. Scammers use these attractive offers to lure victims into providing personal and financial information.

If dealing with a property management company, research its reputation. Legitimate companies have a traceable history and a positive online presence. Avoid those with limited information or negative reviews.

When making rental payments or deposits, use secure and traceable payment methods. Avoid wire transfers or cash transactions, as they offer little recourse in case of fraud.

Request and verify the credentials of the landlord or property owner. Scammers may impersonate property owners to exploit prospective tenants. Legitimate landlords will provide verifiable contact information and identification.

Pay attention to red flags, such as demands for payment before a lease is signed, requests for personal or financial information upfront or reluctance to provide clear and detailed rental agreements.

REVERSE MORTGAGE SCAMS

Reverse mortgages are available to homeowners over the age of 62 as a way of gaining income from their home equity. While this in itself is not a scam, there are those who target seniors claiming to offer reverse mortgages or to help seniors access their equity but are actually either stealing the money or committing deed fraud to steal the home.

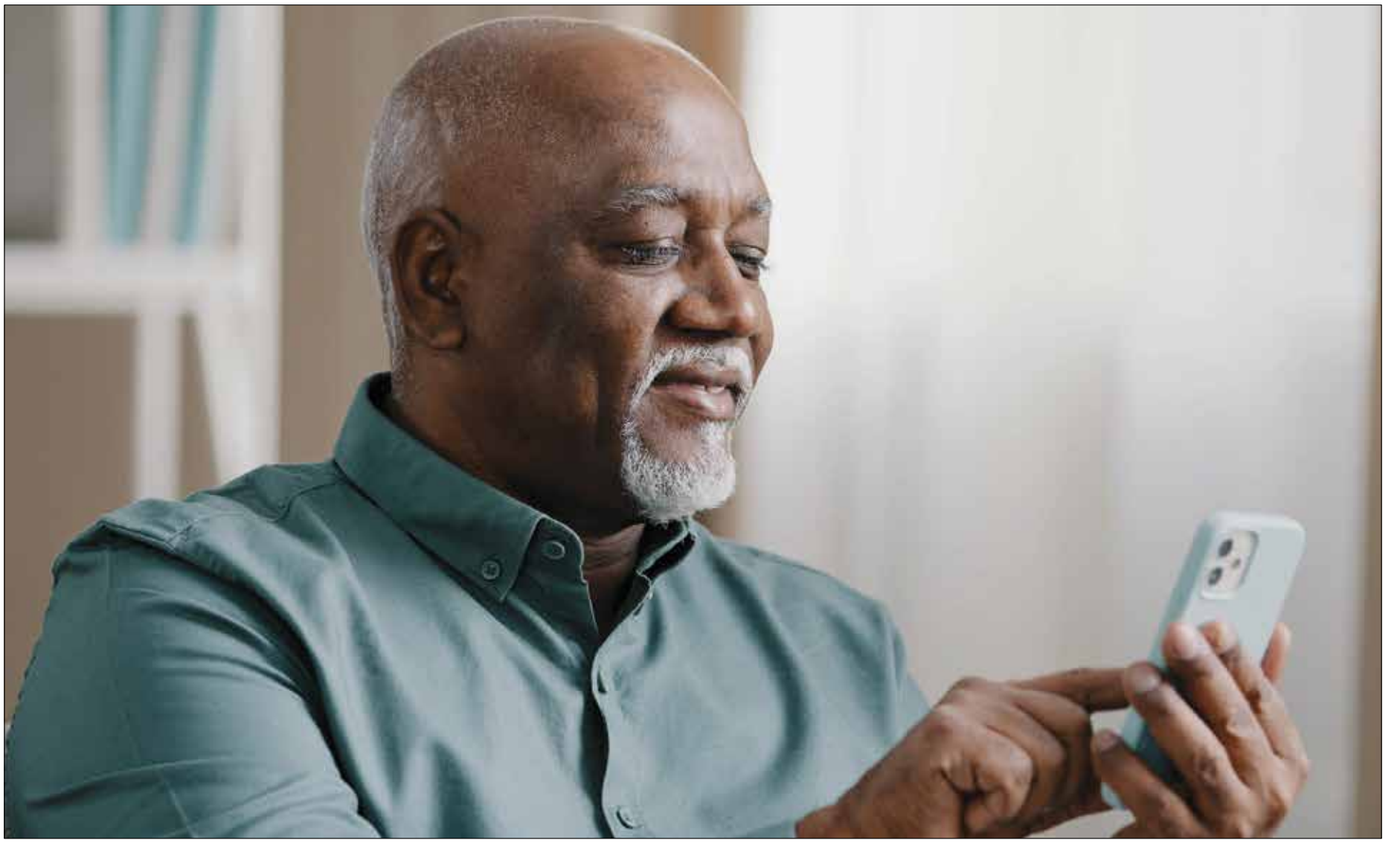
Other variations, according to Aura, a security firm, are fraudsters offering seniors fast approval on a reverse mortgage to avoid foreclosure in exchange for an upfront fee and fraudulent contractors who come to a senior's home offering free consultations and convincing homeowners to take out a reverse mortgage to pay for unnecessary repairs and updates on the home.

Before engaging in a reverse mortgage, verify the credentials of the lender. Ensure they are reputable and licensed to provide such financial products. Understand the terms and conditions of a reverse mortgage. Seek independent advice from financial professionals to ensure you comprehend the risks and benefits.

Scammers may use high-pressure tactics to push seniors into hasty decisions. Be wary of anyone urging you to sign documents quickly or discouraging you from seeking independent advice. Rely on trusted resources for information on reverse mortgages, such as government agencies, reputable financial institutions and legitimate financial advisors.

Recognizing Email Scams

Email interconnects us all, an integral part of communication for people of all ages, including seniors.



© ADOBE STOCK

Unfortunately, with the convenience of email comes the risk of falling prey to phishing scams. Seniors, in particular, may be more vulnerable to these deceptive tactics.

Phishing is a cybercrime where the perpetrator tries to get sensitive information from the target such as user names, passwords, credit card details or other personal information, usually by posing as someone trustworthy. It usually happens over email, but can also happen over social media, instant messaging or phone calls.

The National Council on Aging describes some common phishing attempts being those who start with a pleas for help, "you're the grand prize winner," your bank account has been compromised or the government is after you.

RECOGNIZING PHISHING EMAILS

Carefully inspect the sender's email address. Phishers often use deceptive addresses that may appear legitimate at first glance. Scrutinize the sender's email domain for any irregularities or misspellings.

Phishing emails often contain spelling and grammatical errors. Be cautious if you notice any language inconsistencies or awkward phrasing in the email content. Legitimate organizations typically maintain a professional standard in their communication.

Do not open unexpected attachments or click on links within emails. Genuine organizations usually communicate important information through secure channels. Verify the legitimacy of attachments and links to avoid falling into phishing traps.

Phishers often create a sense of urgency or fear to manipulate recipients into taking immediate action. Be wary of emails that make threats or pressure you to provide sensitive information or make quick decisions without proper verification.

AVOIDING PHISHING SCAMS

Enable two-factor authentication whenever possible. Two-factor authentication adds an extra layer of security by requiring a second form of verification, such as a code sent to their mobile device, before accessing sensitive accounts.

Be aware of tactics employed by phishers, such as pretending to be a trusted entity or using emotional appeals. Double-check with known contacts or organizations if you receive suspicious requests.

Do not give out personal information over emails or confirm sensitive data such as bank account numbers, Social Security numbers, addresses or phone numbers. Do not give out personal information on a phone call if the person called you.

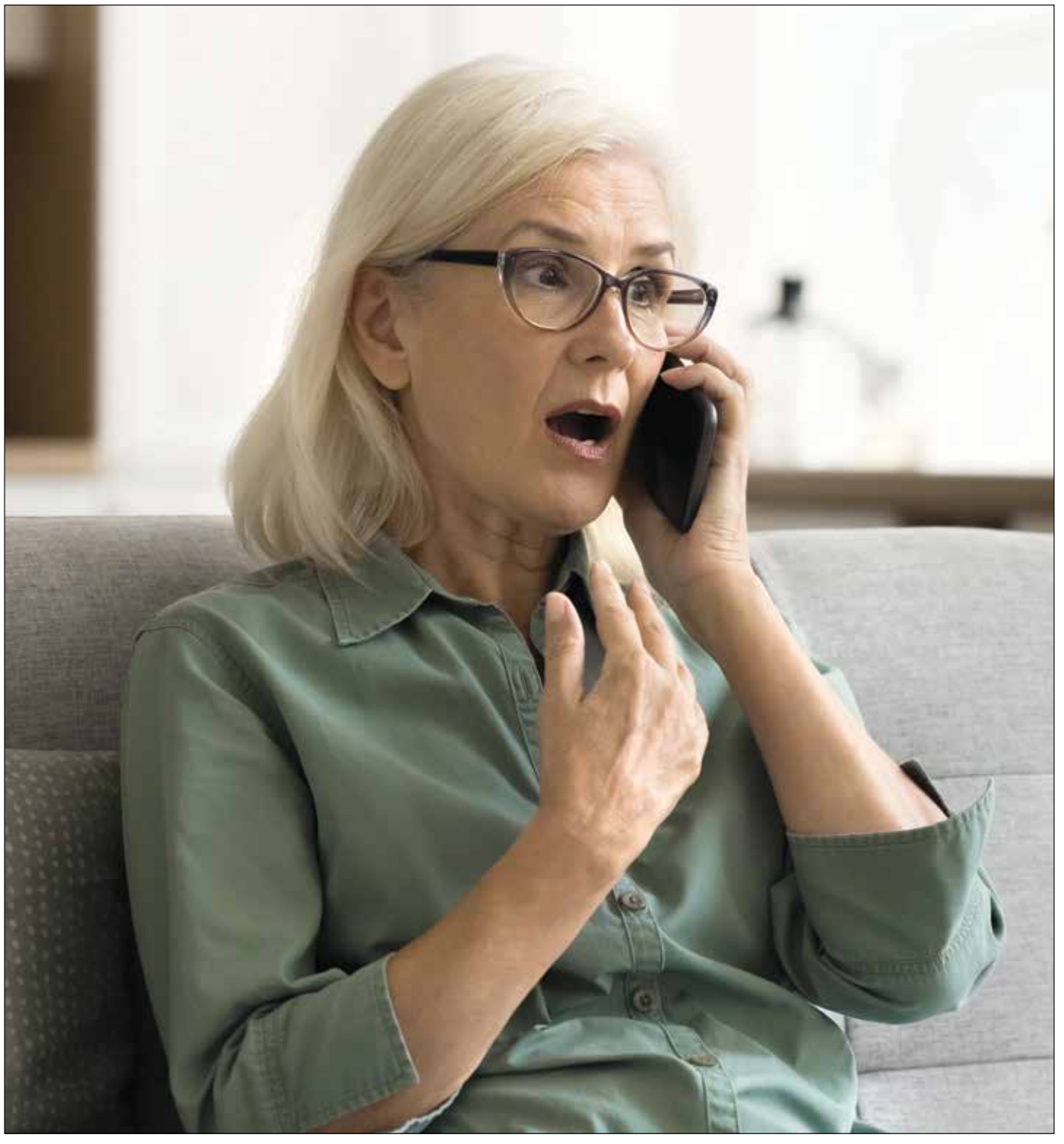
Do not click on links to websites. Instead, type in the direct URL to the website you want to visit.

Keep your devices and security software up-to-date. Regular updates often include patches for potential vulnerabilities, protecting you from the latest phishing techniques.

In an era where technology plays a crucial role in daily life, equip yourself with the knowledge to navigate the digital landscape safely. By understanding the signs of phishing emails and adopting proactive measures, seniors can significantly reduce their risk of falling victim to scams.

Unraveling Grandparent Scams

Every grandparent worries about the safety of their grandchildren. It's instinctual to immediately try to help them if they're reaching out to you because they are in trouble. Unfortunately, that is something fraudsters take advantage of.



© ADOBE STOCK

Scams have become increasingly sophisticated, preying on trusting individuals. One particularly heart-wrenching scheme is the "grandparent scam," where the instigators pose as distressed grandchildren seeking urgent financial assistance.

The Federal Trade Commission reported that in 2022, American seniors who were victims of fraud — nearly half a million seniors — lost an average of $1,000 to $1,800 each.

The grandparent scam typically unfolds with a phone call from an individual claiming to be your grandchild. They may present a scenario of being in a dire situation, such as involvement in a car accident, in legal trouble or stranded in a foreign country. The caller often pleads for immediate financial aid, urging you not to disclose the situation to their parents for fear of repercussions.

The first and most crucial step is to remain calm. Scammers rely on instigating panic to cloud judgment. Politely ask the caller questions only your grandchild would know, such as specific family details, childhood memories, or shared experiences. They'll try to trick you into saying the grandchild's name so they can use it, so if someone calls saying, "Hi, Grandpa, it's your granddaughter!" an answer might be, "Which one?" even if you have only one.

Request to speak directly with your grandchild. Be cautious if the caller avoids this request or offers excuses for being unable to talk. Legitimate family members would readily comply with such a simple request. If the situation seems urgent, hang up and independently contact your grandchild or other family members to verify the claims. Use trusted phone numbers, not those provided by the caller. Scammers often provide alternative contact information to prevent you from seeking confirmation.

Refrain from transferring funds or providing sensitive information over the phone. Scammers commonly pressure victims to act swiftly, using urgency as a tool to exploit emotions. Take time to verify the authenticity of the situation before making any financial decisions.

Check the legitimacy of the caller's story with other family members or friends. Scammers often employ high-pressure tactics, making it difficult to think rationally. Confirming the details independently can help uncover inconsistencies and reveal the scam. Embrace technology to protect yourself. Scammers often target seniors due to a perceived lack of familiarity with digital tools. Consider using video calls or other forms of communication to visually verify the caller's identity.

Share your experiences and newfound knowledge about grandparent scams with friends and fellow seniors. Awareness is a powerful tool in preventing these schemes from succeeding. Encourage open conversations about potential scams within your community.

Stay vigilant, stay informed and stay safe.

Spot Tech Support Scams

In an era dominated by technology, scammers are finding new and insidious ways to exploit unsuspecting individuals.

© ADOBE STOCK

Seniors are often particularly vulnerable to their tactics. One prevalent scheme that continues to target seniors is the tech support scam, one that starts with an unexpected call or message from someone claiming to be a tech support representative.

Tech support scams typically begin with a cold call or a pop-up message claiming to be from a reputable tech company. The caller, often posing as a representative from a well-known tech giant, asserts that your computer has been infected with a virus or malware. The urgency of the situation is emphasized, creating a sense of panic and prompting immediate action.

RED FLAGS

Be wary of unexpected calls or messages from alleged tech support representatives. Legitimate tech companies rarely initiate contact unless you have first called them with a request and they are returning the call. Scammers often use high-pressure tactics, insisting on immediate action to fix the purported issue. They may claim that failure to comply could result in severe consequences, such as data loss or identity theft.

Tech support scammers commonly request remote access to your computer. Legitimate tech support representatives from reputable companies would never ask for unsolicited access to your device.

Be cautious if the caller demands payment for their services. Tech support from reputable companies does not involve upfront fees or unexpected charges.

HOW TO HANDLE UNEXPECTED CALLS OR MESSAGES

The first line of defense is to remain calm. Scammers capitalize on panic to manipulate victims. Take a deep breath and approach the situation with a clear mind. Politely ask for the caller's name, company and contact details. Verify this information independently before taking any further action. Legitimate tech support representatives will provide this information willingly.

Under no circumstances should you grant remote access to your computer to an unsolicited caller. This provides scammers with the opportunity to install malicious software or access sensitive information. If you have doubts about the legitimacy of the call, hang up immediately. Do not engage in further conversation or provide any personal information. Trust your instincts and prioritize your safety.

If you are genuinely concerned about your computer's security, contact the official tech support channel of the company in question using verified contact information. This ensures you are dealing with legitimate professionals. Stay informed about common scams and educate fellow seniors about the tactics employed by scammers. Awareness is a powerful tool in preventing these schemes from succeeding.