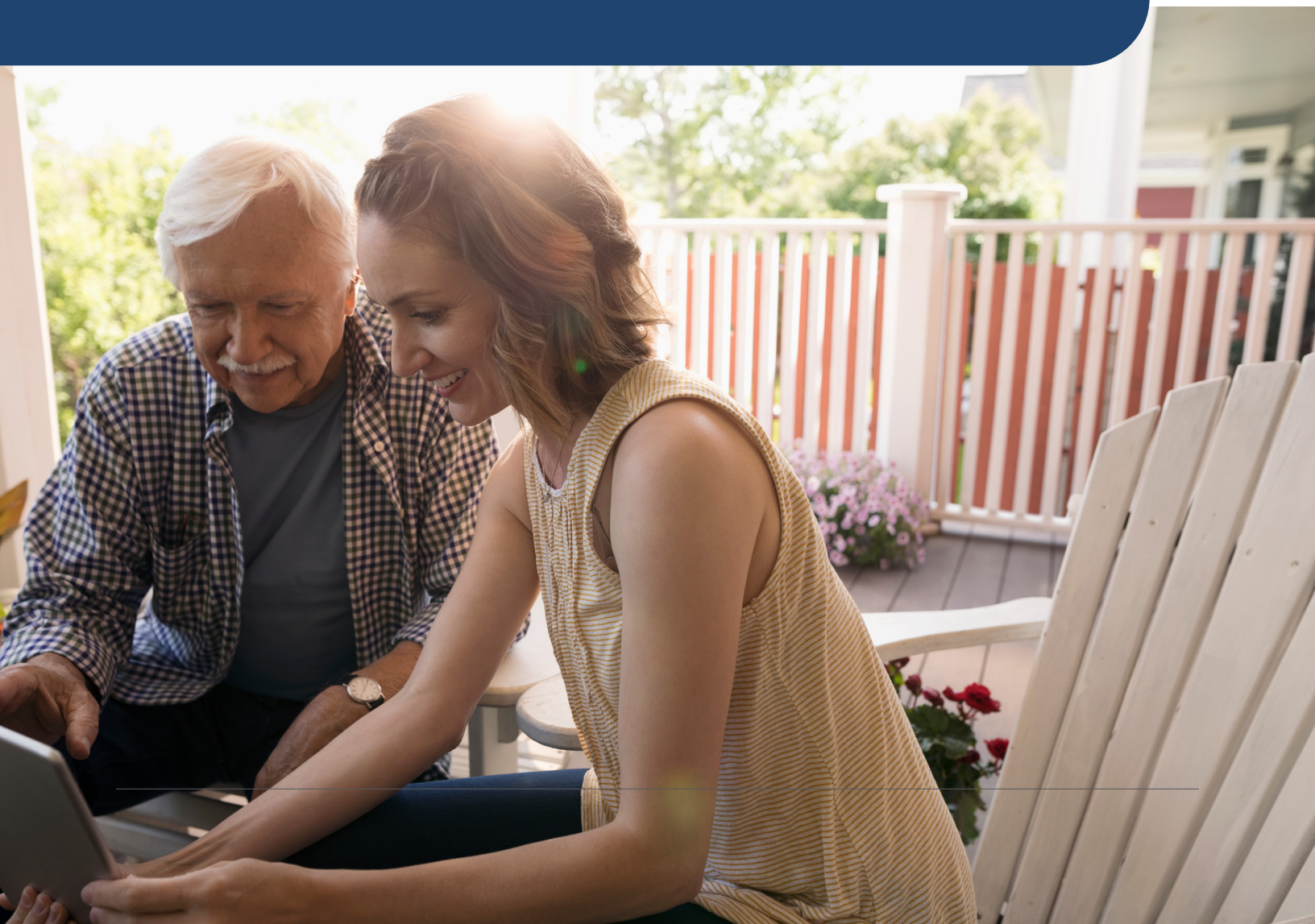
Helping Silver Surfers Navigate Online

Scamming the elderly is a multibillion-dollar business that drains seniors of their retirement funds and government benefits. Bad actors do not discriminate. They take from all regardless of race, rich or poor, healthy or ailing[1]. Recent estimates from the United States Federal Bureau of Investigation (FBI)[2] indicate that elderly people lose about $3 billion to scammers every year. And less conservative estimates project seniors lose up to $36 billion annually[3].



Top elderly scams

Malware
Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system. It is commonly downloaded through phishing emails, or from the internet or USB drives / removable media.

Ransomware
This is a type of malware that encrypts your files (i.e. photos, personal files, tax documents, etc). The bad actor freezes your device and demands payment from you to restore access to your data.

Fake sweepstakes or lotteries

A lottery scam is a type of advance-fee fraud which begins with an unexpected email notification, phone call, or mailing often claiming that you have won a large sum of money or prize.

Counterfeit prescription drugs
Fake medicine that contains the wrong or inactive ingredient. It is produced and sold with the intent to take advantage of the consumer.

Counterfeit drugs are illegal and may be harmful to your health. For more information click here.

Pop-up ads peddling fake anti-aging products
Fake pop-up advertising can include phone numbers to call, reputable brand names you recognize and initiate unsolicited noise while your surfing the internet. Avoid clicking on these ads that open in a separate window, advertise free or heavily discounted products and services, and can potentially enable others to capture your personal information and/or maliciously steal your money or download malware.

Sweetheart scams
Online dating is common practice today to help one find romance. Be cautious of people who appear too good to be true, ask for personal information or request money. Make sure you investigate the dating site before you create a profile.

Fake credit card scams
There are many scammers out there trying to make a quick buck. Many will pose as credit card issuers, suggesting that your personal information needs to be updated for one reason or another all to gain access to your assets. Tip: Never give out personal information over the phone or in an email to people or company's you do not know or have not called yourself. When in doubt, hang up and then contact the company directly through a trusted website or phone number.

Employment scams
Job and employment scams trick individuals into handing over their money in return for a "guaranteed" way to make fast money with little effort.

Phony free vacations
Be on the look out for travel scams because they are out there. Before booking your next adventure, check out these 10 red flags that could be a possible travel scam.

What seniors can do to prevent being scammed:

Manage their transactions
Never make unusual money transfers without discussing with a friend or relative. Without exception, talk to someone first. Criminals will pressure seniors through urgency, greed, curiosity or fear and prevent them from talking to someone else before making a decision.

Don't give away personal information
Consult family members and caregivers about potential purchases before going through with them. Never give away information on an impulse unless you are positive it's to a trusted source, for example, a doctor or company you've done business with before.

Watch for too-good-to-be-true scams
If a deal on a vacation, prescription drug, or anything else seems too good to be true, it probably is. Research the company offering the deal.

Don't fall for bad actors
If someone is trying to sell something to you or get more information out of you, ask for verification about who they represent. If they refuse, walk away or hang up the phone. No offer is that time sensitive. You can always go back and research the offer on your own.

Know that the government will only notify you by mail
For example, the U.S. government never uses email or website ads to notify you of an infraction or collect personal information from you.

Keep travel plans off the internet

Don't post your vacation travel plans, location or agenda on social media until after you return. You don't want to publicize that you have an empty house.

What you can do to protect your seniors

Individuals are still the first line of defense for stopping fraud against senior citizens. You can help keep the elderly safe with these actions:

Be your seniors "safe place"
Foster a relationship of gentle trust. Seniors may feel reluctant to give up control and therefore, keep secrets about decisions or certain arrangements. Keep them informed of the latest scams. Let them know that you are there to offer help, understanding and not to take over or judge. This will hopefully lead to an open dialog that can give you the insight necessary to protect them effectively.

Regularly call or visit seniors
Be suspicious if a senior citizen has a new "best friend", becomes socially isolated, never seems to be available or able to come to the phone, or is hesitant to have contact with others unless a caregiver is present. This could indicate that someone has undue influence on the senior's behavior and decision-making. Try to encourage your friend to always chat through money ideas and transactions with you first. Telling someone before the transaction will help a lot.

Block solicitations

- Opt-out of commercial mail solicitations.
- To eliminate unsolicited offers for credit, go to Opt Out Prescreen
- Tools for controlling mail, email and telephonic direct marketing contacts

Provide relief for caregivers
Caregiving can be very taxing on the heart and the mind. They say it takes a village to raise a child. That is no less true for caregiving for a senior in need.

Set up safeguards at the bank
If you're concerned about your relative's financial decision-making, set up a small account at a local bank for them.

Arrange for limited account oversight
Ask financial institutions to send statements and alerts to a trusted person who has no direct access to the senior's accounts, so that person can check for fraud.

Keep loved ones informed
Let seniors know they could be scammed on the internet through things like emails and pop-up ads. It is good to remember that if is seem to good to be true, it probably is.

Check seniors' bank accounts regularly
Check your loved one's bank accounts and retirement accounts often with an eye for odd purchases or withdrawals.

Visit seniors to discuss their monthly bills and prescriptions
They may mention a "new" bill or a "cheaper" way to get the prescriptions they need in passing, so follow up on any of those.

Make sure your loved ones know not to make any impulse online buys
Pay special attention to a "deal" ending in the next few minutes.

Be mindful of family and friends
Although we want to believe that most people have good intentions, it is often family members or friends that will take advantage of ailing seniors.

How to report scams and cyber crime

More than 80 percent of online scams go unreported, partly because people don't know how or where to report them. Learn more.

Reporting Resources:

Banking and Retirement Fraud *(Contact your bank/retirement facility immediately)*

Scams of the elderly often involve money coming from bank or retirement accounts. As soon as you discover that you or someone you know has been scammed, notify whomever deals with the account. You might still have a chance to recover your money, or it might not have left the account yet.

Cyber Crime

- The Internet Crime Complaint Center (IC3)
  IC3 is a partnership between the Federal Bureau of Investigation and the National White Collar Crime Center. Complaints may be filed online. Keep in mind, you will need to contact your credit card company directly to notify them if you are disputing unauthorized charges on your card or if you suspect that your credit card number has been compromised.
- Federal Bureau of Investigations (FBI)
  The FBI deals with blue- and white-collar crimes and will investigate online scams, especially if money is involved.

Cyberbullying

If you suspect that someone is being cyberbullied: Find out details about the activity and report it here.

Foreign company complaints

EConsumer.gov accepts complaints about online and related transactions with foreign companies.

Identity Theft

If you have been a victim of identity theft, report it here.

Investment Scams

Securities and Exchange Commission (SEC) If you've "invested" in an opportunity that you later suspect is a scam, report it to the SEC.

National Center For Missing and Exploited Children – Cyber Tipline.

Online Business/Shopping Scams

Better Business Bureau (BBB)
If you suspect a business is scamming you online, report it to the Better Business Bureau. A map on their website identifies businesses all over the country that have tried to scam people in person and on the web.

Phishing and Telemarketing Scams

Federal Trade Commission (FTC)
The FTC shares consumer complaints covering a wide range of categories, including online scams, with local, state, federal, and foreign law enforcement partners. It cannot resolve individual complaints, but can give you information on the next steps to take. File a complaint here.

Social Security Fraud

The Office of the Inspector General (OIG) is the best p ce to report Social Security fraud. Learn mo bout SS Fraud. Don't Ignore the Fraud. Speak Up.

Learn more about keeping your family safe online

Staysafeonline.com

Download tip sheets, lesson plans and other safety resources

Cyberbullying, sexting, social networking, and more

U.S. Federal Trade Commission's main resource to educate consumers on staying safe and secure online

Cybersecurity and Infrastructure Security Agency (CISA)

Concerned Parent's Internet Safety Toolbox

Identity Theft Resources

National Do Not Call List – Action: Register your phones

Local Victim Service Provider – Most communities in the United States have victim advocates ready to help following a crime. Find local victims service providers here.

Global Resources:

Children Helpline International

EMEAR National Society for the Prevention of Cruelty to Children (NSPCC)

EMEAR Secure Internet Centre (SIC)

APJC Go safe online

Homeland Security

UNICEF East Asia – Child Protection in the digital age

[1,3] *agingInPlace*

[2] *https://www.ncoa.org/article/top-10-financial-scams-targeting-seniors*