LEARN

Lifelong Education & Aging Resource Network



Scam Savvy Seniors

Empowering Seniors in the Digital Age

IDAHO Community Care Program

Case Management - Advocacy - Respite - Education

Importance of Awareness: Protecting Yourself and Your Loved Ones



1 Increased Security

Knowing about scams helps you identify potential threats and take precautions.

2 Protecting Finances

Awareness helps you avoid falling victim to scams that target your money and savings.

3 Protecting Identity

Learning about common scams can help you safeguard your personal information.

4 Emotional Well-being

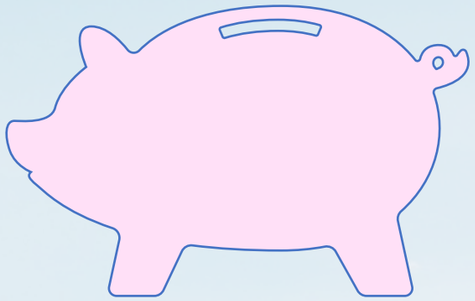
Knowing about these tactics helps you avoid the emotional distress of becoming a victim.

Why Seniors Are Targeted?



Perceived Wealth

Scammers assume seniors have substantial savings and assets. They target retirement funds and home equity.



Politeness

Many older adults feel uncomfortable hanging up on callers. Scammers exploit this kindness.



Lack of Tech Familiarity

Some seniors are less familiar with evolving digital threats. This can make them more vulnerable.





Three Golden Rules of Scam Spotting

1

Slow It Down

Never rush decisions when money is involved

2

Spot Check

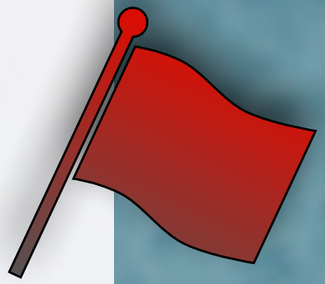
Verify information through official channels

3

Stop! Don't Send!

No legitimate business demands gift cards as payment

Recognizing Scam Red Flags



1 **Urgency**

Scammers create panic to push quick actions. Don't let them rush you.

2 **Personal Information Requests**

Legitimate organizations rarely ask for sensitive data via email or phone. Be cautious.

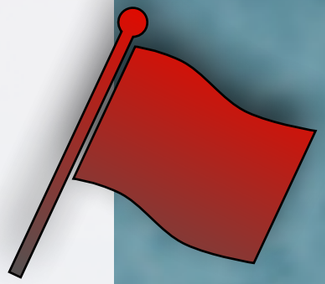
3 **Unsolicited Contact**

Contact out of the blue through calls, emails, texts or direct messages on social media.

4 **Too Good To Be True**

If an offer seems unrealistically beneficial, it probably is. Trust your instincts.

Recognizing Scam Red Flags



5 **Unusual Payment Methods**

Gift cards or cryptocurrency requests are often scams. Stick to trusted payment methods.

6 **Impersonation**

Pretending to be from reputable organizations, like banks, government agencies, companies.

7 **Emotional Manipulation**

Exploiting emotions such as fear, guilt, love, or sympathy to gain compliance.

8 **Poor Written Communication**

Generic greetings, spelling errors, or awkward phrasing can indicate a scam.

Recognizing Scam Red Flags

9 **Request for Secrecy**

You’re urged to not tell anyone, claiming confidentiality is necessary.

10 **Inconsistent or Unverifiable Details**

Scammers provide value or changing information, avoiding specifics when questioned.

11 **Fake Confirmations or Alerts**

Claims you’ve made a purchase or your account has been compromised.

12 **Threats, Intimidation**

They may threaten you with arrest, deportation, or legal action to coerce payment or information.



Recognizing Scam Red Flags

13 **Asking for too much Information**

Scammers ask for excessive details that aren’t relevant.

14 **Weird Website Address or Email Addresses**

Scams often use links or email addresses that closely mimic legitimate ones.

15 **Fake Contact or No Contact Details**

Scammers rarely provide reliable ways to reach them.





Phishing Scams Exposed

1

The Bait

Scammers send fake emails (or text messages, even calls) posing as legitimate organizations. They create convincing replicas.

2

The Hook

Urgent messages claim account issues. They pressure you to act quickly.

3

The Catch

Clicking links leads to fake websites. These steal your login credentials or personal information.

Once scammers have your information, they can access your accounts, make unauthorized purchases, or steal your identity.

Recognizing Phishing Email Red Flags



Urgent Action Required

Scammers create a sense of urgency to pressure you into acting without thinking clearly.



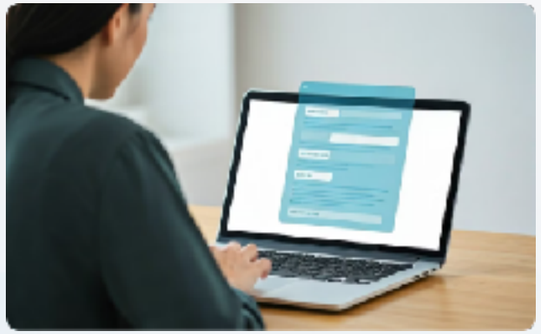
Unusual Sender Address

Be cautious of misspellings in domains or unfamiliar email addresses.



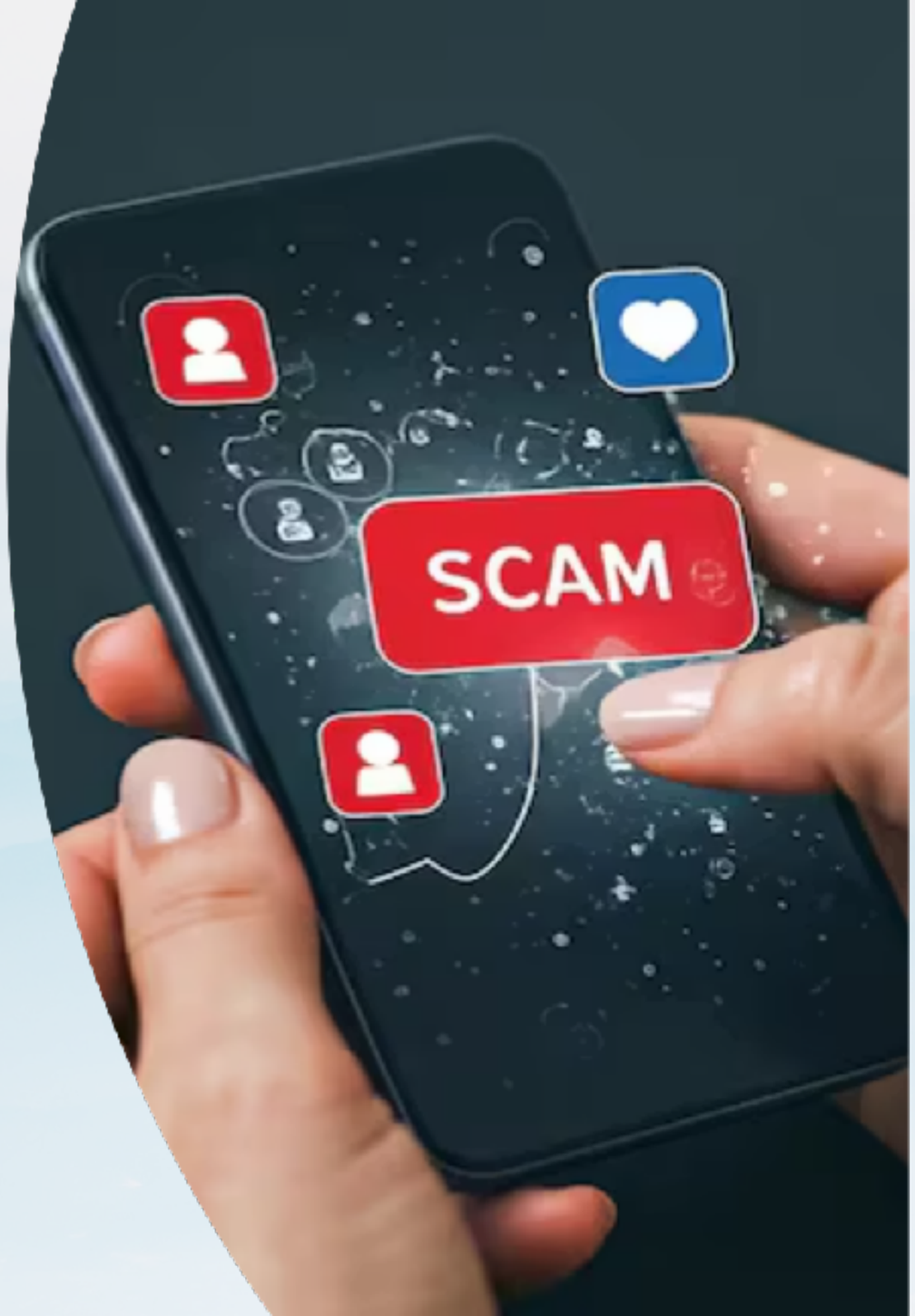
Requests for Personal Information

Legitimate companies won’t ask for sensitive information like passwords or bank details through email.



Poor Grammar and Spelling

Many scam emails contain obvious language mistakes, a red flag indicating their illegitimate nature.



Medicare and Social Security Fraud

1

Initial Contact

Scammers pose as officials via phone or email. They claim urgent benefit issues.

2

Information Gathering

They request personal details to "update" records. This information is used for identity theft.

3

Fraudulent Activity

Scammers use stolen info to bill for fake services. They may also redirect your benefits.



Tech Support Pop-Up Scams

1

The Setup

Pop-up warnings or calls claim your computer is infected. They offer immediate "help".

2

The Trick

Scammers demand you call a phone number . Or they request remote access to your computer. They pretend to fix non-existent problems.

3

The Theft

Once inside, they steal personal data or install malware. They may also charge for fake services.

1 Aggressive Phone Calls

Scammers often use threatening language and claim you owe back taxes, demanding immediate payment to avoid arrest or legal action.

2 Spoofed Caller ID

They may use technology to make their calls appear to come from legitimate IRS phone numbers, increasing their credibility.

3 Unusual Payment Methods

Unlike the real IRS, scammers typically demand payment through gift cards, wire transfers, or cryptocurrencies.

4 Lack of Due Process

The real IRS will always provide taxpayers with the opportunity to question or appeal the amount owed before requesting payment.



Investment Fraud: Beware of Get-Rich-Quick Schemes

Scammers often lure people with promises of quick and easy riches through investments. Remember, if it sounds too good to be true, it probably is.

High Returns	Promising unrealistic returns on investment.
Guarantees	Offering guaranteed profits without disclosing risks.
Pressure	Pressuring you to invest immediately without proper research.
Limited Information	Providing little to no information about the investment.





Charity Scams: Exploiting Generosity

How It Works

Fake charities exploit generosity for personal gain

Red Flags

High-pressure tactics, vague mission statements

Stay Safe

Verify legitimacy before donating



Sweepstakes Scams: You Never Really Won

How It Works

Fake prize notifications requiring upfront payments

Creates excitement about "winning" something valuable

Red Flags

Requests for fees or taxes upfront

Prizes for contests you never entered

Pressure to act quickly

Stay Safe

Be skeptical of unsolicited winnings

Never send money to claim a prize

Legitimate prizes don't require payment



Grandparent Scams: The Emotional Trap

How It Works

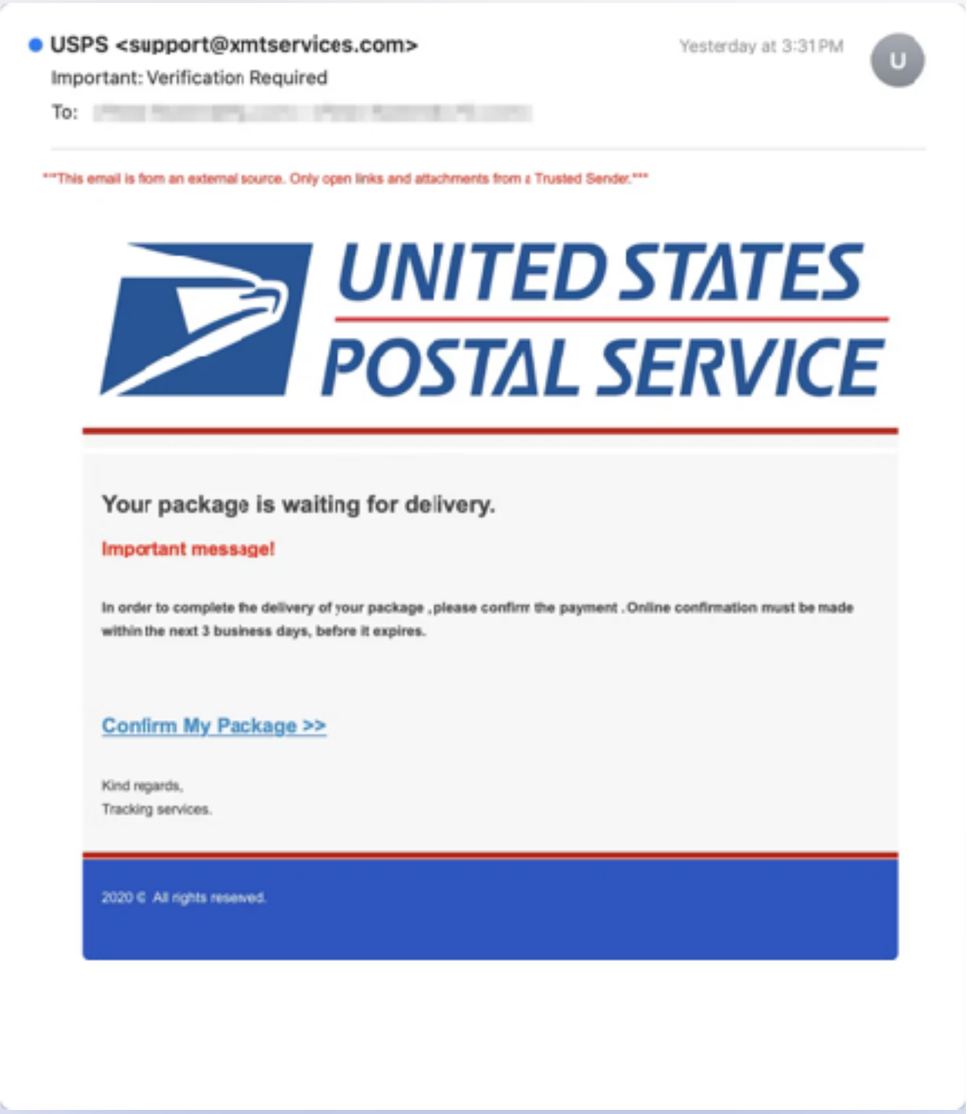
Scammers pose as grandchildren in urgent trouble

Red Flags

Immediate cash requests, unusual details in story

Stay Safe

Verify with family before sending money



Fake Confirmations or Alerts

Deceptive Messages

Scammers send fake order or account alerts with urgent language.

Warning Signs

Look for incorrect sender addresses, spelling mistakes, and suspicious links.

Stay Safe

Never click links in unexpected alerts. Verify through official channels.

Report Suspicious Activity

Tell your security team about any questionable communications.

Romance Scams: Love Lies

1

Initial Contact

Attractive profile, quick declarations of love

2

Building Trust

Daily communication, personal stories, deepening relationship

3

The Ask

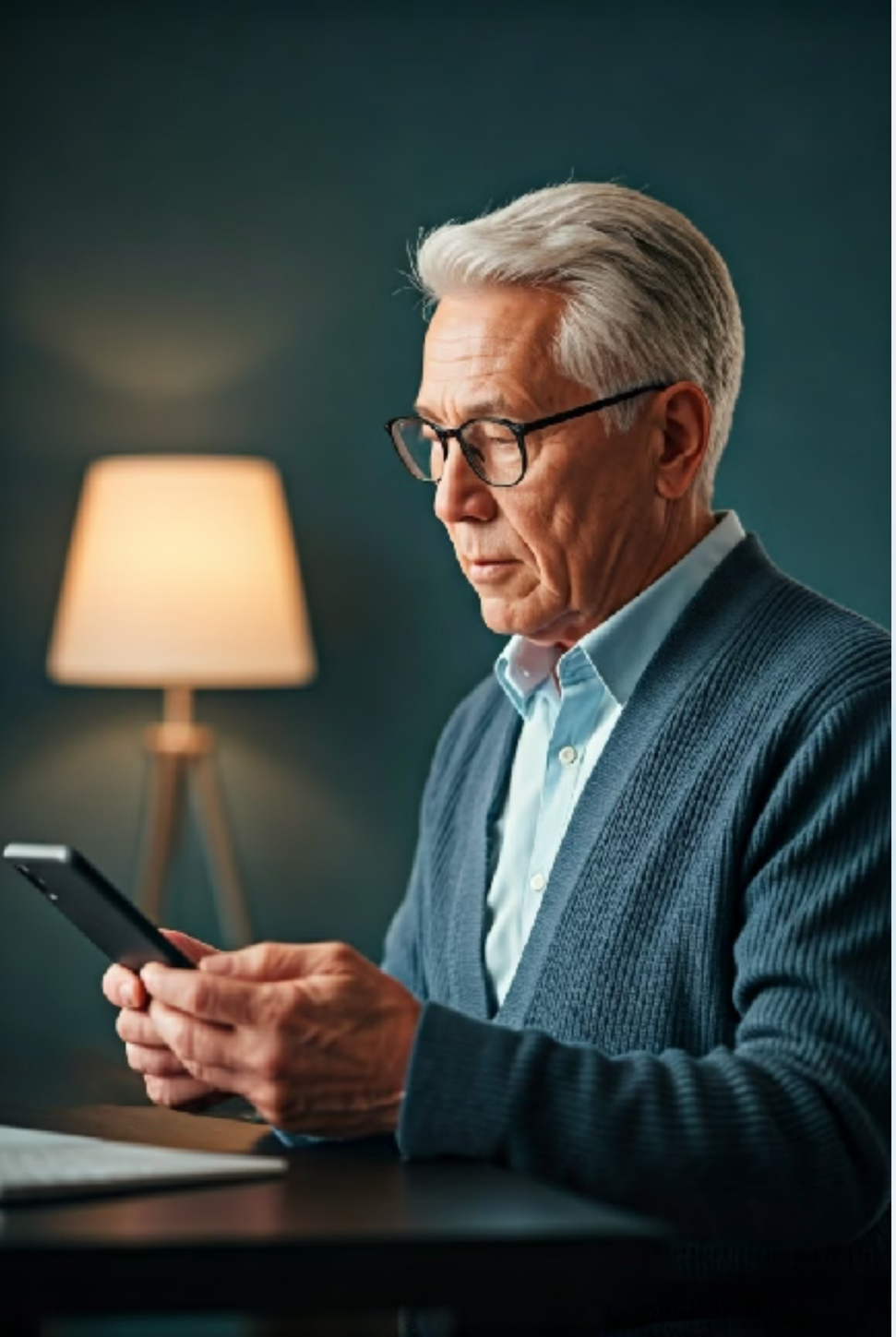
Emergency situation, requests for money transfer

4

Continuous Demands

More emergencies, larger money requests





Staying Safe on Social Media

Privacy Settings

Adjust your account to limit public information. Review settings regularly.

Friend Requests

Only accept requests from people you know. Be cautious of duplicate accounts.

Sharing Wisely

Think twice before posting personal information. Avoid sharing travel plans publicly.

Secure Login

Use two-factor authentication when available. It adds an extra layer of security.

Identity Theft Scams

Identity theft scams can have far-reaching consequences, potentially impacting your finances, credit score, and personal reputation. These scams involve stealing your personal information to commit fraud or other crimes in your name.

Common Tactics

- Phishing emails and fake websites
- Dumpster diving for personal documents
- Stealing mail or credit card offers
- Data breaches of companies you do business with

Warning Signs

- Unexpected charges on your credit card
- Bills for accounts you didn't open
- Calls from debt collectors about unfamiliar debts
- Errors on your credit report



Identity Theft: Safeguarding Your Personal Information

1

Protecting Your Information

Shred documents with sensitive information and be cautious about sharing personal details online or over the phone.

2

Monitoring Your Accounts

Regularly check your credit reports and bank statements for any suspicious activity.

3

Freezing Your Credit

Consider freezing your credit to prevent unauthorized accounts from being opened in your name.

4

Reporting Identity Theft

If you suspect identity theft, report it immediately to the authorities and the credit bureaus.



Gift Cards as Payment

Gift Cards as Payment

Scammers often request gift cards for various reasons.

Red Flags

Legitimate businesses don’t accept gift cards for payment.

Untraceable Funds

Gift cards offer scammers an easy way to access funds.



Threats or Intimidation

Respond Calmly

Take a moment to check facts before acting

Recognize Red Flags

Demands for unusual payment methods signal fraud

Remember the Truth

Legitimate organizations won't use threats or pressure

Scammers create fear with threats of arrest, fines, or account closure. They demand immediate payment through wire transfers, gift cards, or cryptocurrency.



What to Do If You're Scammed

1

Act Quickly

Contact your bank immediately to freeze accounts. Change passwords for all online accounts.

2

Report the Scam

File reports with local police and the FTC. Provide as much detail as possible.

3

Seek Support

Don't be ashamed to tell friends and family. They can help you recover.

4

Monitor Credit

Place a fraud alert on your credit reports. Watch for any suspicious activity.

Fraud Alerts & Credit Freezes: What's the Difference?



Looking for ways to protect your identity? Here are two options to consider.

Fraud Alert

- ☑ Makes lenders verify your identity before granting new credit in your name. (Usually, they'll call you to verify your identity.)
- ☑ Free
- ☑ Available to anyone who is or suspects they may be affected by identity theft
- ☑ Lasts one year
- ☑ To place: Contact **one** of the three credit bureaus. That bureau must tell the other two.

Credit Freeze

- ☑ Restricts access to your credit report to help prevent identity theft. (Usually, you'll need a PIN or password to place or lift the freeze.)
- ☑ Free
- ☑ Available to anyone
- ☑ Lasts until you lift it
- ☑ To place or lift: Contact **all three** credit bureaus. (If you know which bureau a lender will use, you can lift for only that one.)

How do I contact the credit bureaus?

To place a fraud alert or credit freeze, here's where to go:

Equifax	Equifax.com/personal/credit-report-services 800-685-1111
Experian	Experian.com/help 888-EXPERIAN (888-397-3742)
TransUnion	TransUnion.com/credit-help 888-909-8872

Resources for Reporting Scams

Federal Trade Commission (FTC)

Report online scams to the FTC. You can file a complaint online or by phone.

AARP Fraud Watch Network

The AARP Fraud Watch Network helps older adults protect themselves from scams.

IC3 (FBI's Internet Crime Complaint Center)

The FBI's Internet Crime Complaint Center (IC3) takes reports of internet crimes, including scams.

Idaho Office of the Attorney General - Consumer Protection

Idaho Department of Finance - Consumer Affairs

Local Law Enforcement



Protect Yourself: Key Takeaways

Verify claims directly	Use official contact details only
Avoid clicking unknown links	Never download suspicious attachments
Use secure payment methods	Gift cards are never for bill payment
Stay informed about scams	Share knowledge with friends and family
Trust your instincts	If something feels wrong, it probably is



LEARN

Lifelong Education & Aging Resource Network



IDAHO Community Care Program

Case Management - Advocacy - Respite - Education

Providing statewide information, support, and education to caregivers, family, and other loved ones taking care of an individual with memory concerns, dementia, or Alzheimer's.

www.a3ssa.com/community-care-program