

How to Avoid a Scam

- Do not allow anyone but a trusted family member, friend, or professional financial adviser to handle your personal finances or banking.
- Never give out your PIN, social security number, bank account, Medicare, or credit card over the phone, unless you have initiated contact and know the company that you are speaking to.
- Never send this information via email. Do not toss any documentation that includes this type of information in the trash. Shred these types of documents.
- Use precautions with your financial information online. Shop with retailers that are well-known companies. If you are making an online purchase, make sure the website is safe—review their privacy policy and make sure they use encryption (look for lock symbol). And if you must create a password, make sure it is at least eight characters long and includes some upper- and lower-case letters, numbers, and special characters.
- Sign up for identity theft protection to monitor personal and financial information. If there is an issue, this type of protection can provide aid and assistance to an individual.
- Get recommendations from friends or family for reputable help or services, such as gardening, housekeeping, or meal prep, who may be entering your home. When using an in-home care provider, work with the VA or an established agency, or request references and get a background check if you are personally hiring someone.
- Be careful of door-to-door sales. Most reputable companies no longer use this practice.
- Be cautious of high-pressure sales pitches with too much urgency. Slow down and do not feel threatened to act immediately.
- Never sign a contract without clearly understanding the terms of the agreement. Be skeptical of free trial offers and be sure you clearly understand their cancellation policy.
- Use precautions with your financial information online. Shop with retailers that are well-known companies.