HANDBOOK FOR SENIORS

# Savvy Saving Seniors®

## Steps to Avoiding Scams

Bank of America

ncoa National Council on Aging

WISER Women's Institute for a Secure Retirement

# Contents

# *Quiz:* How Much Do You Know about Scams?

1. **If there's only a small amount of money involved, it's probably not a scam.**
   a. True
   b. False

2. **A company offering to rescue your home from foreclosure may be running a scam if it:**
   a. Says it will stop the foreclosure from taking place.
   b. Suggests that you transfer ownership of the home to the company, so you can rent and buy the property back from them.
   c. Advises you to stop talking to your lender, lawyer, or housing counselor.
   d. All of the above.

3. **Credit-based scams only occur when someone contacts you.**
   a. True
   b. False

4. **One way to tell whether a website offers security to help protect your sensitive data is:**
   a. A small yellow lock appears at the bottom of the browser window.
   b. Your friends shop on the website all the time and never have a problem.
   c. You heard about the website through an online search engine.
   d. The security certificate for the site matches the name of the site.

5. **If you get an email from a federal government agency such as the IRS or the FDIC asking you to confirm or prove personal financial information, it's always safe to do so.**
   a. True
   b. False

6. **If you think you've been tricked by an internet scam, you should:**
   a. Report it to the company whose email address or website was forged.
   b. Change the passwords on all your accounts.
   c. Check your financial statements immediately.
   d. All of the above.

7. **You've just realized that your ATM/debit card has been lost or stolen. To get the maximum legal protection against losses from unauthorized withdrawals, you should notify your bank:**

   a. Immediately or as soon as you discover your card is missing.

   b. Within 10 business days.

   c. Before your next statement arrives, even if it's weeks later.

8. **Your credit report may suggest that you've been a victim of identity theft if it shows:**

   a. You have a credit card, loan, or lease in your name that you know you don't have.

   b. A company you never tried to do business with has requested a copy of your credit report.

   c. A home address for you that you never had.

   d. All of the above.

9. **It's safe to enter personal or financial information into pop-up windows on websites.**

   a. True

   b. False

**10. The usual suspects who might want to scam me include:**

a. Strangers

b. Family members

c. Caregivers

d. All of the above

## Quiz Answers:

1. **False.** No matter how much money is involved, you should always be alert for a scam.

2. **(d) All of the above.** Many homeowners who are having difficulty making their monthly mortgage payments are being targeted by criminals who falsely claim they can rescue a home from foreclosure, then charge large upfront fees and fail to deliver on their promises. In some of the worst cases, homeowners are tricked into signing away ownership of their house.

3. **False.** Credit-based scams on the Internet are on the rise. It can happen when you are seeking credit loans online as well. Be aware when entering applications online.

4. **(d)** The security certificate for the site matches the name of the site. Seeing the yellow lock icon is a good sign because the closed lock icon signifies that the website uses encryption to help protect any sensitive or personal information that you enter. To ensure it's genuine, double-click on it to view the security certificate for the site. The name following **"Issued to"** should match the name of the site. If the name differs, you may be on a fake site, also referred to as a "spoofed" site. If you're not sure whether a certificate is real, don't enter any personal information. Play it safe and leave.

5. **False.** Just because an email or website looks like what you'd expect from a government agency, remember that there are convincing copycats out there. The IRS, other government agencies, your bank would never contact you online to ask for personal information such as account numbers and online passwords and usernames.

6. (d) **All of the above.** The best thing you can do after being tricked by an internet scam is to keep an eye on all of your accounts, alert the proper parties, and change your passwords so that no one can access your information. Learn more about improving password security from Better Money Habits®. *http://go.bofa.com/539h6*

7. (a) Immediately or as soon as you discover your card is missing. Under the Electronic Fund Transfer Act, if your debit card or ATM card is lost or stolen, your maximum liability is limited to $50 if you notify your bank within 2 business days of discovering that the card is missing. If you wait more than 2 business days but no more than 60 days after receiving a bank statement that includes an unauthorized transfer, you could be liable for losses up to $500. But if you wait longer than that, the law doesn't require your bank to reimburse you for any unauthorized transfers made after the 60-day period, even if that would clean out your account. **Note:** After you report a lost or stolen card, under most circumstances you will limit your responsibility for unauthorized transactions from that point on.

8. **(d) All of the above.** There are many good reasons to frequently review your credit reports, and one is to look for warning signs that an identity thief has been or is trying to obtain loans or commit other fraud in your name. The most important warning sign of ID theft in a credit report is a credit card, loan, or lease in your name that you know nothing about. Any one of these may indicate that someone has learned enough information about you to be able to steal your identity and conduct business acting as you. Also pay close attention to the "inquiries" section of the report that shows who has requested a copy of your credit history. That's because thieves sometimes falsely claim to represent a company with a lawful right to obtain credit reports and then use the information to commit fraud.

9. **False.** It is not safe to enter personal or financial information into pop-up windows on the web. One common internet scam technique is to launch a fake pop-up window when someone clicks a link in an email message. It can look very convincing and might be displayed over a window you trust. Even if the pop-up window looks official or claims to be secure, you should avoid entering sensitive information because there is no way to check the security certificate.

10. **(d) All of the above.** Sadly, elders need to be careful of all the individuals in their life as potential financial abusers. This does not mean you need to isolate yourself from those who care about you, but it does mean you need to be alert to the motivations and actions of those around you. Keep an eye on your accounts and limit access to these accounts.

# Top 10 Scams Targeting Seniors

1. **Health Care/Medicare/Health Insurance Fraud:** Every U.S. citizen or permanent resident over age 65 qualifies for Medicare, so there is rarely any need for a scam artist to research what private health insurance company older people have in order to scam them out of some money.

2. **Counterfeit Prescription Drugs:** Counterfeit drug scams operate on the Internet where seniors increasingly go to find better prices on specialized medications. This scam is growing in popularity—since 2000, the FDA has investigated an average of 20 such cases per year, up from five a year in the 1990s.

3. **Funeral & Cemetery Scams:** The FBI warns about two types of funeral and cemetery fraud perpetrated on seniors. In one approach, scammers read obituaries and call or attend the funeral service of a complete stranger to take advantage of the grieving widow or widower. Claiming the deceased had an outstanding debt with them. Another tactic of untrustworthy funeral homes is to bank on family members' unfamiliarity with the considerable cost of funeral services to add unnecessary charges to the bill.

4. **Fraudulent Anti-Aging Products:** Whether it's fake Botox like the one in Arizona that netted its distributors (who were convicted and jailed in 2006) $1.5 million in barely a year, or completely bogus homeopathic remedies that do absolutely nothing, there is money in the anti-aging business. These scams can drain resources and sometimes a bad batch can have health consequences.

5. **Telemarketing:** Perhaps the most common scheme is when scammers use fake telemarketing calls. With no face-to-face interaction, and no paper trail, these scams are incredibly hard to trace. Once a successful deal has been made, the buyer's name is then shared with similar schemers looking for easy targets, sometimes defrauding the same person repeatedly.

6. **Internet Fraud:** Internet scams that are everywhere on the web. Pop-up browser windows simulating virus-scanning software will fool victims into either downloading a fake anti-virus program (at a substantial cost) or an actual virus that will open up whatever information is on the user's computer to scammers.

7. **Investment Schemes:** From pyramid schemes like Bernie Madoff's (which counted a number of senior citizens among its victims) to fables of a Nigerian prince looking for a partner to claim inheritance money to complex financial products that many economists don't even understand, investment schemes have long been a successful way to take advantage of older people.

8. **Homeowner/Reverse Mortgage Scams:** Scammers like to take advantage of the fact that many people above a certain age own their homes, a valuable asset that increases the potential dollar value of a certain scam. For trusted information on reverse mortgages and consumer protections, we encourage seniors to visit *www.ncoa.org/homeequity.*

9. **Sweepstakes & Lottery Scams:** Scammers inform their mark that they have won a lottery or sweepstakes of some kind and need to make some sort of payment to unlock the supposed prize. Often, seniors will be sent a check that they can deposit in their bank account, knowing that while it shows up in their account immediately, it will take a few days before the (fake) check is rejected. During that time, the criminals will quickly collect money for supposed fees or taxes on the prize, which they pocket while the victim has the "prize money" removed from his or her account as soon as the check bounces.

10. **The Grandparent Scam:** The Grandparent Scam is so simple and so underhanded because it uses one of older adults' most reliable assets, their hearts. Scammers will place a call to an older person and when the mark picks up, they will say something along the lines of: "Hi Grandma, do you know who this is?" When the unsuspecting grandparent guesses the name of the grandchild the scammer most sounds like, the scammer has established a fake identity. Once "in," the fake grandchild will usually ask for money to solve some unexpected financial problem, to be paid via Western Union or MoneyGram, which don't always require identification to collect.

# Tips for Avoiding Scams

## Top 8 Ways to Protect Yourself

1. Be aware that you are at risk from strangers—and from persons closest to you.
2. Do not isolate yourself—stay involved with friends, family, and community activities!
3. Always tell salespeople that come to your door or call you on the phone: "I never buy from (or give to) anyone who calls or visits me unannounced. Please send me your information in writing."
4. Shred all receipts with your credit card number.
5. Sign up for the "Do Not Call" list (*www.donotcall.gov*) to prevent telemarketers from calling and take yourself off multiple mailing lists. Phone: 1-888-382-1222
6. Use direct deposit for benefit checks to prevent checks from being stolen from the mailbox.
7. Never give your credit card, banking, Social Security, Medicare, or personal information over the phone unless you initiated the call.
8. Be skeptical of all unrequested offers and thoroughly do your research if you're seeking any type of services. Also be sure to get references when possible.

## Tips for Avoiding Telemarketing Fraud

It's very difficult to get your money back if you've been cheated over the telephone. Before you buy anything by telephone, remember:

- **Don't buy from an unfamiliar company.** Reasonable businesses understand that you want more information about their company and are happy to comply.
- **Always ask for and wait until you receive written material about any offer or charity.** If you get brochures about costly investments, ask someone whose financial advice you trust to review them. But, unfortunately, beware—not everything written down is true.
- **Always check out unfamiliar companies.** Check them with your local consumer protection agency, Better Business Bureau, state attorney general, National Fraud Information Center, or other watchdog group. Unfortunately, not all bad businesses can be identified through these organizations.
- **Obtain a salesperson's detailed information.** Ask for their name, business identity, telephone number, street address, mailing address, and business license number before you transact business. Some con artists give out false names, telephone numbers, addresses, and business license numbers. Verify the accuracy of these items.

- **Find out where your money will go.** Before you give money to a charity or make an investment, find out what portion of the money is paid in commissions and what portion actually goes to the charity or investment.
- **Look for a guarantee.** Before you send money, ask yourself a simple question: "What guarantee do I really have that this salesperson will use my money in the manner we agreed upon?"
- **Don't pay in advance for services.** Pay services only after they are delivered.
- **Be cautious of companies that want to send a messenger to your home.** Some fraudulent companies want to send someone to pick up money, claiming it's part of their service to you. In reality, they are taking your money without leaving any trace of who they are or where they can be reached.
- **Always take your time making a decision.** Reasonable companies won't pressure you to make a snap decision.
- **Don't pay for a "free prize."** If a caller tells you the payment is for taxes, he or she is violating federal law.
- **Know your limits.** Before you receive your next sales pitch, decide what your limits are—the kinds of financial information you will and won't give out on the telephone.

- **Wait, think, and discuss before you decide.** Be sure to talk over big investments offered by telephone salespeople with a trusted friend, family member, or financial advisor. It's never rude to wait and think about an offer.
- **If you don't understand, don't respond.** Never respond to an offer you don't understand thoroughly.
- **Know who you're dealing with.** Never send money or give out personal information such as credit card numbers and expiration dates, bank account numbers, dates of birth, or Social Security numbers to unfamiliar companies or unknown persons.
- **Realize your information is shared.** Be aware that your personal information is often brokered to telemarketers through third parties.
- **Be cautious of help with losses.** If you've been victimized once, be wary of persons who call offering to help you recover your losses for a fee paid in advance.
- **Always report fraud.** If you have information about a fraud, report it immediately to state, local, or federal law enforcement agencies.

**REMEMBER: If it sounds too good to be true, it probably is!**

Learn more from Better Money Habits® about how to recognize an offer that's too good to be true. *http://go.bofa.com/9bchk*

## Tips for Protecting Your Identity

Many people don't realize how many different ways identity thieves can obtain personal information, nor how easy it is for them to do it. Here's how to protect yourself:

- **Monitor your bank and credit card statements.** Check your accounts regularly, so you can catch any purchases made on your credit card by persons other than yourself. The same goes for cash withdrawals.

- **Do not fall for internet scams.** Understand what internet scams are and don't respond to any attempts. Do not click on the links in the emails.

- **Beware of telephone scams.** Never give out personal information over the phone to someone who claims to represent your bank, credit card company, or other organization. People are not always who they claim to be.

- **Be careful with your mail.** Sometimes identity thieves will steal your mail right out of your mailbox in order to obtain your personal identifying information. To reduce this threat, try not to let incoming mail sit in your mailbox for a long time. If you're going to be away for extended periods of time, have the post office hold your mail for you. When sending out sensitive mail, consider dropping it off at a secure collection box or at the post office.

- **Be careful when using account information in public.** Whether punching in your PIN number at an ATM or filling out forms with personal information on it, be sure to cover the keypad or complete paperwork in as private a setting as possible. Also, don't give out credit card information over the phone in a public place when, for example, making travel reservations. Make those calls in private.

- **If you suspect that you have been a victim of identity theft:**

  1. Contact your bank(s) and credit card companies immediately.

  2. File a report with the police. The police may not be able to do very much themselves, but companies you work with to clear up identity theft issues may want to see a copy of this report.

  3. Put out a fraud alert to the credit-reporting agencies:
     a. Experian: 1-888-397-3742 (TDD 1-800-972-0322)
     b. Equifax: 1-888-766-0008 (TDD 1-800-255-0056 and request connection to Auto Disclosure Line at 1-800-685-1111)
     c. Transunion: 1-800-680-7289 (TDD 1-877-553-7803)

# Protecting Yourself and Loved Ones from Scams

Financial abuse and scams are serious concerns. They deprive older people of their hard-earned assets and retirement savings. Making matters worse, seniors, with limited incomes and earning potential, are rarely able to recover financially.

Everyone is subject to scams and con games. But because older people are identified as easy marks, they are frequently targeted by the dishonest. Many times, the scammers are strangers preying upon older individuals who may be lonely, isolated, confused, or desperate for cash or attention.

There are also many instances of financial abuse where the scammers are family members. Sometimes, the victim is pressured into giving money or assets to a family member or friend claiming to need financial assistance.

Older people may feel a sense of duty to help family members, or might do so out of fear of the person whom they rely on for care. Experts say this kind of financial abuse by friends and family members often goes unreported.

It's important for you to be on the lookout, not only to protect your assets, but also to help you identify possible scams against yourself, family members, and friends.

## Protect Your Loved Ones: Signs to Look For

- A large amount missing from their bank or other cash accounts.
- Numerous withdrawals of smaller amounts—such as $100 at a time.
- A large check written to someone you don't know.
- A change in their power of attorney or the beneficiaries on their insurance or investment accounts.
- Bouncing checks or bills going unpaid when there should be enough money in their account to cover their needs.
- Unusual or unnecessary purchases—such as buying new golf clubs or a diamond bracelet.
- Unnecessary home repairs—such as having new siding put on the house or the driveway repaved.
- Becoming close with a much younger person or inappropriate person.
- A caregiver who becomes overly interested in the person's finances or who will not allow others access to the older adult.
- Older adult suddenly appears confused, unkempt, or afraid.
- Piled up sweepstakes mailings, magazine subscriptions, or "free gifts."

# Additional Scam Scenarios

## Work-at-Home Scams:

Frequently in the classifieds or on job listing websites, there are jobs that sound easy and promise to bring in lots of money, usually all from the comfort of working in your own home. However, what usually happens is that individuals are then required to pay up front for training, equipment, or "starter kits." If you ever have to pay money upfront, the odds are good that it's a scam, and you will never make the bundles of money promised. Common jobs listed that wind up taking your money instead of earning you money are:

- Data entry done from home
- Stuffing envelopes
- Starting an online business
- Posting ads
- Secret Shopper

## Jury Scams:

Another example of fraud is an email or phone call about jury duty saying you missed your appearance and asking for your Social Security number in order to confirm your information.

# If You or Someone You Love is a Victim of Financial Fraud or Abuse

Don't be afraid or embarrassed to talk about it with someone you trust. You are not alone, and there are people who can help. Doing nothing could only make it worse. Keep handy the phone numbers and resources you can turn to, including the local police, your bank (if money has been taken from your accounts), and Adult Protective Services.

To obtain the contact information for Adult Protective Services in your area, call the Eldercare Locator, a government-sponsored national resource line, at 1-800-677-1116, or visit their website at *www.eldercare.gov.*

# Helpful Resources

### Credit Reports:

*www.AnnualCreditReport.com*

### Federal Trade Commission:

*www.ftc.gov/idtheft*

*www.ftc.gov/phonefraud*

*www.ftc.gov/moneymatters*

### Protection against Fraud:

*www.OnGuardOnline.gov*

*www.DoNotCall.gov*

1-888-382-1222

### Social Security Fraud Hotline:

1-800-269-0271

### FBI's Internet Crime Complaint Center:

*www.ic3.gov*

### Better Business Bureau:

*www.bbb.org*

### Better Money Habits®:

In collaboration with several nonprofits, Bank of America has produced Better Money Habits® to help people who are living paycheck to paycheck stabilize and improve their financial situations. Visit *BetterMoneyHabits.com* to find videos, infographics and articles about building an emergency fund, managing bills, handling overdue debts, and more.

# Organizations with Resources on Scams & Fraud

**Consumer Financial Protection Bureau:**
*www.consumerfinance.gov*

**Consumer Federation of America:**
*www.consumerfed.org*

**Elder Financial Protection Network:**
*www.elderfinancialprotection.org*

**FINRA Investor Education Foundation:**
*www.saveandinvest.org*

**Justice in Aging:**
*www.nsclc.org*

**National Consumer League's Fraud Center:**
*www.fraud.org*

**National Consumer Protection Technical Resource Center' Senior Medicare Patrol:**
*www.smpresource.org*

**Women's Institute for Secure Retirement:**
*www.wiserwomen.org*

# Useful Links for Savvy Saving Seniors

### Administration on Aging's National Center on Elder Abuse:

*www.ncea.aoa.gov*

### BenefitsCheckUp®:

*www.BenefitsCheckUp.org*

1-888-268-6706

### Eldercare Locator:

*www.eldercare.gov*

1-800-677-1116

### Food Bank Search:

*www.feedingamerica.org*

### IRS Volunteer Income Tax Assistance Program:

*www.irs.gov*

### My Medicare Matters:

*www.mymedicarematters.org*

### Home Equity Advisor:

*www.homeequityadvisor.org*

### National Council on Aging:

*www.ncoa.org/savvyseniors*

### National Foundation for Credit Counseling:

*www.nfcc.org*

1-800-388-2227

### Senior Community Service Employment Program:

*www.dolta.gov/seniors*

### Supplemental Nutrition Assistance Program—Food Stamps:

*www.fns.usda.gov*


National Council on Aging

251 18th Street South • Suite 500 • Arlington, VA 22202
571-527-3900 • ncoa.org • @NCOAging