Lesson 5: Avoiding Fraud and Scams

Topics to be Covered

“As I grow older, I pay less attention to what people say. I just watch what they do.” – Andrew Carnegie

Health Strategies
⇒ Health Fraud
⇒ Red Flags

Wealth Strategies
⇒ Funeral and Cemetery Fraud
⇒ Telemarketing Scams
⇒ Identity Theft
⇒ Charity Scams
⇒ ATM Machines
⇒ Senior “Specialists” and Advisors
⇒ Investment Fraud
⇒ Tips to Avoid Investment Fraud
⇒ Reporting Scams

Objectives

Learning Objectives
- Participants will learn about health fraud and how to protect themselves.
- Participants will learn key signs to identifying health fraud and reporting procedures.
- Participants will learn about different types of financial scams that specifically target seniors.
- Participants will learn key signs to identifying financial scams and how to protect themselves.

Behavioral Objectives
- Participants will be informed regarding health and financial fraud.
- Participants will be able to identify fraud red flags.

Background Information

Fraud complaints have increased sharply over the last decade. This increase was likely fueled by the internet and economic conditions. According to the Federal Trade Commission (FTC), consumer financial losses per capita have increased as well. In fact, the median loss per victim rose from $218 in 2002 to $537 in 2011 (Blanton, 2012). Consumers reported paying over $1.7 billion for fraud complaints (Blanton, 2012). The take-home message is to always trust your instincts, ask for more information, take your time, check for credibility, and run it by a trusted loved one or advisor.
Top 10 Scams Targeting Seniors

The top 10 scams targeting seniors include (NCOA, 2013):
1. Health Care/Medicare/Health Insurance Fraud
2. Counterfeit Prescription Drugs
3. Funeral & Cemetery Scams
4. Fraudulent Anti-Aging Products
5. Telemarketing
6. Internet Fraud
7. Investment Schemes
8. Homeowner/Reverse Mortgage Scams
9. Sweepstakes & Lottery Scams
10. The Grandparent Scam

Health Strategies

HEALTH FRAUD
✓ Health fraud is defined by the FDS as “the deceptive promotion, advertising, distribution, or sale of a product represented as being effective to prevent, diagnose, treat, cure, or lesson an illness or condition, or provide another beneficial effect on health, but that has not been scientifically proven safe and effective for such purposes”.
✓ We have all seen these “miracle” weight loss supplements or natural remedies that claim to “cure” arthritis.
✓ Most of these products focus on “quick fixes” to complex health issues, when in reality they are only trying to sell a product.
✓ Health fraud scams may target the elderly through infomercials and commercials on TV, direct mail, and magazines.

✓ Make sure to always consult your health care provider before taking ANY medications, especially supplements that you found on your own.
✓ Taking small steps to becoming aware can help you avoid these fraudulent products.
✓ If it sounds too good to be true, it probably is and you shouldn’t fall for it.
✓ If the product claims to cure many different unrelated diseases, you shouldn’t fall for it.
✓ If there are testimonials by famous people, actors, “doctors,” or “real people” that tell you how amazing the product is, you shouldn’t fall for it (FDA, Don’t be a Victim).

RED FLAGS TO RECOGNIZING SCAMS
According to the FDA, key red flags to look for are words like:
- Miraculous Cure
- Quick Fix
- Ancient Remedy
- New Discovery
- Scientific Breakthrough
- Secret Ingredient
- Natural Cure
- Shrinks Tumors
- Lowers Blood Sugar
- Quick and Painless Cure
- No-Risk Money Back Guarantee

Unfortunately, there are many different types of financial scams out there in addition to health products that can be harmful to you.
Wealth Strategies

FUNERAL AND CEMETERY FRAUD
Given the emotional nature of people during this difficult time, they may become more vulnerable to scams. It is important to make sure that someone who is trustworthy and not as emotionally involved is keeping an eye on the finances.

- Funeral homes are required to provide detailed list of prices over the phone and in writing, if requested.
- Make sure that you call or shop around to at least a few funeral homes to make sure that the prices are reasonable.
- For direct cremation, caskets are not required and embalming is not legally required.
- If you choose to pre-pay for funeral services, make an educated decision and shop around. Be sure to keep copies of all paperwork with your other important documents.

TELEMARKETING SCAMS
These scams are frequently targeted towards the elderly who may be home alone (FBI). Here are some small steps you can take to be on the guard against scams:

- Examples include receiving phone calls telling us that we have won a prize from a contest or sweepstakes, a free vacation, or we need a home repair or need to send money right away.
- Always be wary of any giveaways or sales pitches over the telephone. Reputable businesses will always be willing to provide you with more information to prove their legitimacy and will respect your wariness.
- If you are interested in the offer and it seems legitimate, always ask for more information and time to make your decision.
- If it is a “limited time offer,” it’s probably a scam. If you receive any written materials, make sure to show them to your loved ones and financial advisors for accuracy. Don’t be afraid to look up any organization on the internet to check its credentials.
- Don’t pay for any services before they are offered to you. Also, if someone offers you a “free prize” but says that you have to pay for taxes, they are violating the law (FBI).
- Be aware and question the offer. If businesses just gave away free prizes, they wouldn’t be very profitable.

IDENTITY THEFT
According to the Federal Trade Commission, Florida has the highest per capita rate of reported identity complaints followed by Arizona and California. Identity theft is also a growing concern that can be financially disastrous.

Identity theft occurs when someone takes your personal information and uses it as if it was their own, usually to open credit card accounts or make other financial purchases.

- Do not share personal identifying information such as your Social Security number or date of birth.
- It is important to keep in mind that identity theft is not only committed by strangers, but also often by someone close to us who may be going through some financial hardship (Institute for Financial Literacy, 2010).
Wealth Strategies

CHARITY SCAMS
If you're considering making a donation to a charity, do some research before you give.

✓ Make sure to ask for paperwork from the organization legitimizing their existence and their 501(c) tax-exempt status.
✓ Know the difference between “tax exempt” and “tax deductible.” Tax exempt means the organization doesn’t have to pay taxes. Tax deductible means may be able to deduct your contribution on your federal income tax return.
✓ Ask for detailed information about the charity including name, address, and telephone number.
✓ Call the charity. Ask if the organization is aware of the solicitation and has authorized the use of its name.
✓ The organization may have a website and promotional materials, but that does not necessarily mean they are a legitimate charity.
✓ Be wary of charities that spring up too suddenly in response to current events and natural disasters.
✓ Ask how much of your donation actually goes to the cause.
✓ Never send cash donations or wire money to someone claiming to be a charity.
✓ You can contact your local Better Business Bureau to assist you in verifying a charity.

ATM MACHINES
✓ It is always very important to be aware of your surroundings when withdrawing money from an ATM machine.
✓ Make sure to use only ATM machines from a reputable bank or credit union and check your bank statements each month for fraudulent charges.
✓ If the ATM area is not secure, someone can gain access to your account information and be able to withdraw from it.

“SENIOR” SPECIALISTS AND ADVISORS
✓ Some financial professionals use designations such as “senior specialist” or “retirement advisor” to imply that they are experts at helping seniors with financial issues.
✓ The education, experience, and other requirements for receiving and maintaining a “senior” designation vary greatly.
✓ Look beyond a financial professional’s designation and determine whether he or she can provide the type of financial services or product you need.
✓ Thoroughly evaluate the background of anyone with whom you intend to do business—before you hand over your hard-earned cash.
Wealth Strategies

INVESTMENT FRAUD

✓ “Ponzi” and pyramid schemes
  ◆ These investment scams are essentially “robbing one person to pay another.” Initial investors are paid off with money taken from new investors.

✓ Oil and gas scams
  ◆ If you think you’ve found the right oil or gas investment to “strike it rich,” consider this: it may be a scam.

✓ Promissory notes
  ◆ A promissory note is a form of debt—similar to a loan or an IOU—that a company may issue to raise money.
  ◆ While promissory notes can be legitimate investments, those that are marketed broadly to individual investors often turn out to be scams.

✓ Prime bank fraud
  ◆ In a prime bank scheme, fraudsters often claim investors’ funds will be used to purchase and trade “prime bank” financial instruments or other “high yield investment programs” (“HYIPs”) on clandestine overseas markets in order to generate huge returns in which the investor will share.
  ◆ However, neither these instruments, nor the markets on which they allegedly trade, exist.

✓ High return or “risk free” investments
  ◆ Some unscrupulous investment advisors make unsuitable recommendations to purchase investment products that don’t meet the investment objectives or means of an investor.

TIPS TO AVOID INVESTMENT FRAUD

⇒ You can do your best to prevent fraud by being vigilant and aware of your surroundings and be able to recognize false claims.
⇒ The point is to be careful about who you trust and keep good documentation.
⇒ Don’t be afraid to ask questions to clarify things you don’t understand and check out the answers.
⇒ Research the company before you invest
⇒ Know the salesperson
⇒ Never judge a person’s integrity by how he or she sounds
⇒ Watch out for salespeople who prey on your fears
⇒ Take your time—don’t be rushed into investment decisions
⇒ Be wary of unsolicited offers
⇒ Don’t lose sight of your investments
⇒ Question why you cannot retrieve your principal or cash out your profits
⇒ Don’t be afraid to complain

REPORTING SCAMS

✓ To report fraud and scams in Florida, consumers can call 1-800-378-0445.
✓ Also, remember to file a report with your local law enforcement office.
✓ Consumers can file a complaint with the Federal Trade Commission about misleading ads or websites for health products by calling 1-877-FTC-HELP (1-877-382-4357), or visiting ftc.gov/complaint.
✓ SEC: 1-800-732-0330
✓ FINRA BrokerCheck: 1-800-289-9999
✓ State Regulators: 1-202-737-0900
Take Home Messages

You can take small steps to recognize and avoid fraud and scams.

Optional Activities

YOU WILL NEED

✓ Savvy Saving Seniors Quiz: How much do you know about scams?
✓ Savvy Saving Seniors Handout: Tips for Avoiding Scams

INSTRUCTIONS

1. Distribute handouts to participants
2. Ask participants to complete the quiz.
3. Facilitate a discussion on fraud and scams.

DISCUSSION PROMPTS

- If you feel comfortable discussing with the group, has anyone here faced a situation where they were afraid that they were being confronted with a scam or knew someone who had?
- What can you do to be more vigilant against fraud and scams?

Handouts

Savvy Saving Seniors Quiz: How much do you know about scams?
Savvy Saving Seniors Quiz Answer Sheet
Savvy Saving Seniors Handout: Top 10 Scams Targeting Seniors
Savvy Saving Seniors Handout: Tips for Avoiding Scams

References


Food and Drug Administration (FDA). Don’t be a victim of health fraud scams. Retrieved from www.fda.gov/ForConsumers/ProtectYourself/HealthFraud/ucm267638


Additional Resources

Florida – On Guard for Seniors http://www.myfloridacfo.com/onguard

Lesson Authors:

Martie Gillen, Ph.D., MBA, Assistant Professor and Family and Consumer Economics for Older Adults Specialist, Family, Youth and Community Sciences, IFAS/Extension, University of Florida.

Amanda Terminello, BS, Graduate Student, Family, Youth and Community Sciences, IFAS/Extension, University of Florida.

Lesson Reviewers:

Barbara O’Neill, Ph.D., CFP, Professor II and Extension Specialist in Financial Resource Management, Rutgers Cooperative Extension.

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 him or her 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 rely 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 is 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 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 [http://www.ncoa.org/independence-dignity/home-equity.html](http://www.ncoa.org/independence-dignity/home-equity.html) and [www.homeequityadvisor.org](http://www.homeequityadvisor.org)

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 do not always require identification to collect.

Adapted from the NCOA Savvy Senior Handbook.
How Much Do You Know about Scams?

1. If there is only a small amount of money involved, it is 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 is 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 have 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. Within two business days of discovering the card missing.
   b. Within 10 business days.
   c. Before your next statement arrives, even if it has 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 do not 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 is 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

Adapted from the NCOA Savvy Senior Handbook.
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 is 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 are not sure whether a certificate is real, do not enter any personal information. Play it safe and leave.

5. False. Just because an email or website looks like what you would 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.

7. (a) Within two business days of discovering the card 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 two business days of discovering that the card is missing. If you wait more than two 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. However, if you wait longer than that, the law does not 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 is 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.
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 are seeking any type of services. Also, be sure to get references when possible.

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

Adapted from the NCOA Savvy Senior Handbook.
<table>
<thead>
<tr>
<th>Time</th>
<th>Activity/Topic</th>
<th>Materials</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 min. 00:00-00:03</td>
<td>Quote: Use the quote as an icebreaker. Read the quote.</td>
<td>Slides 1-3</td>
</tr>
<tr>
<td></td>
<td><strong>Introduction:</strong> Introduce the topic</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Top 10 scams targeting seniors</strong></td>
<td></td>
</tr>
<tr>
<td>4 min. 00:03-00:07</td>
<td><strong>Health strategies</strong></td>
<td>Slides 4-6</td>
</tr>
<tr>
<td></td>
<td>Health fraud and red flags</td>
<td></td>
</tr>
<tr>
<td>11 min. 00:07-00:18</td>
<td><strong>Wealth strategies</strong></td>
<td>Slides 7-18</td>
</tr>
<tr>
<td></td>
<td>Funeral and cemetery fraud, avoiding telemarketing scams, identity</td>
<td></td>
</tr>
<tr>
<td></td>
<td>theft, charity scams, ATM fraud, “senior” specialists and advisors,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>investment fraud, tips for avoiding investment fraud, and reporting scams</td>
<td></td>
</tr>
<tr>
<td>1 min. 00:18-00:19</td>
<td><strong>Take home message</strong></td>
<td>Slide 19</td>
</tr>
<tr>
<td>8 min. 00:19-00:27</td>
<td><strong>Activities</strong></td>
<td>Slide 20</td>
</tr>
<tr>
<td></td>
<td><em>Savvy Saving Seniors Quiz:</em> How much do you know about scams?</td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Savvy Saving Seniors Handout:</em> Tips for Avoiding Scams</td>
<td></td>
</tr>
<tr>
<td>3 min 00:27-00:30</td>
<td><strong>Questions:</strong> Answer any remaining questions</td>
<td>Slide 21</td>
</tr>
</tbody>
</table>
EVALUATION

Thank you for being a part of this lesson. We hope you enjoyed yourself! Please help us do a better job of serving you by completing this evaluation.

1. How much did you learn from this lesson? Please check only one:
   - Very little
   - Some
   - A lot

2. Do you plan on making changes as a result of participating in this lesson?
   - Yes
   - No

3. If you answered “yes,” please tell us what you plan to do. Check all that apply!
   - I plan to use one of the strategies from this lesson to change a health-related behavior. I plan to ____________________________
   - I plan to use one of the strategies from this lesson to change a personal finance behavior. I plan to ____________________________
   - I plan to share information I learned today with a family member or friend.

4. Comments:
   __________________________________________________________________________
   __________________________________________________________________________

Thank you for completing this form! We look forward to seeing you at our other ENAFS programs!