Financial Scams And The Elderly

Milton Township S.A.L.T. Council

October 14, 2021

Presented by: Arnold H. Shifrin, RPh
Director of Communications
Milton Township S.A.L.T. Council
Email: *ahshifrin@gmail.com*

Milton Township S.A.L.T. Council

- **S**eniors **A**nd **L**aw Enforcement **T**ogether.
- A committee of Milton Township formed in 1997.
- Comprised of volunteers, citizens, and representatives from the sheriff's department, local police departments, fire departments, state's attorney office, and other community agencies.
- The Council's goal is to enhance the quality of life of the elderly. One way of accomplishing this is to educate area seniors about steps they can take to protect themselves from fraud and abuse.

Milton Township Office

- 1492 Main Street; Wheaton, IL 60187
- Tel: 630-668-1616

S.A.L.T. Council Meetings

- Held at 10:00 AM on the 2nd Monday of each month in the Community Room at the Glen Ellyn Police Dept.; 65 S. Park Blvd.; Glen Ellyn, Il 60137. [No meeting held in August.]
- Speaker(s) - current topic of interest.
- Scams report - report from each meeting is posted on the township's website: *miltontownshipsalt.com*.

The *"S.A.L.T. Communicator"* (Quarterly newsletter)

- Mailed to 12,000 township residents in January, April, July, and October of each year.
- Each edition of the newsletter is posted on the township's website.

- **Milton Township Online Resources**
  - A complete list of township resources, including assistance with food, transportation, and housing is available on the township's website.

- **S.A.L.T. Council Annual Auto Inspection**
  - Free auto inspection for seniors to help them prepare for winter driving.
  - Inspection is held on a Saturday in October from 9:00 AM to 12:00 noon at Wheaton Fire Station #1 (Fapp Circle).
  - The 2021 auto inspection was held this past Saturday, October 9. The 2022 auto inspection has not yet been scheduled.

TOP 10 FINANCIAL SCAMS TARGETING THE ELDERLY *

1. **Government Impostor Scam**

   Impostors call potential victims and claim to be from Medicare, the Internal Revenue Service (IRS), or the Social Security Administration (SSA). They may state you have unpaid taxes that are past due and threaten you with arrest or deportation if you don't pay immediately. Or an impostor may say there's a new law that requires you to confirm your Social Security Number and other personal information in order to retain your Medicare benefits.

   If you comply with the caller's request and provide the requested information, your identity will be stolen and you will lose money. Your personal information will be sold to other fraudsters.

   Fraudsters currently have access to technology that enables them to "spoof" telephone calls. As a result, your caller ID may show that a call originated from area code 202 (Washington, D.C.) when, in fact, the call could have originated from anywhere in the world.

* per National Council on Aging (February, 2021)

2. The Grandparent Scam

This scam preys upon the emotions of the elderly. Scammers contact an older person on the phone with a greeting such as “Hi Grandma, do you know who this is?” When the grandparent responds with the name of the grandchild the scammer most sounds like, the scammer knows that a “relationship” with the victim has been established.

The scammer next asks the victim for money he suddenly needs for house or car repairs, jail bond, or doctor, hospital, and legal expenses resulting from a recent car accident.

Victims are told to send money to the scammer via gift card, prepaid debit card, or wire transfer. Once such a remittance is made, the money is lost and cannot be recovered.

Victims are asked not to discuss the matter with the grandchild’s parents.

3. **Medicare Scams**

   You receive a telephone call from someone claiming to be a Medicare representative. You're told that you're now eligible to receive additional medical services and equipment such as a wheelchair, mobile scooter, or portable oxygen tanks at no charge to you. In order to receive these benefits, all you have to do is confirm your Medicare Beneficiary Identification (MBI) number and provide some personal information to the agent.

   Once you provide the requested information, the fraudster bills Medicare for services and medical supplies you never received and pockets the money.

   Review your Medicare Summary Notices from CMS to verify that you received the listed services

4. Computer Tech Support Scams

These scams take advantage of the lack of technical knowledge that seniors have about computers. A pop-up message suddenly appears on your computer screen or cell phone. The message tells you that your device is compromised and needs to be repaired. You're instructed to call a special "support" number for help. When you call the number, the fraudster says he needs remote access to your device to make the repairs and quotes you a price for the repairs.

Once the scammer gains access to your computer or phone, your personal information is in jeopardy. The scammer also has an opportunity to install malware (e.g., malicious software) on your device which makes you vulnerable to identity theft.

If you refuse to pay the fee for the repairs, your computer will be locked and you will not be able to access any programs or files on the hard drive.

5. Sweepstakes and Lottery Scams

You receive an email message stating that you have just won money in a lottery or sweepstakes and that a check for the winnings has been mailed to you. You're told to deposit the check when you receive it and then remit a specified amount to the sender for taxes and fees.

When you receive the check and deposit it in your account, it shows up in the account balance. Feeling secure with the transaction at this point, you send the money for the taxes and fees as requested.

Several days later, the sender's check "bounces" and your account is debited. In the meantime, the sender has collected the money you sent. Thus, you not only didn't win a lottery or sweepstakes contest, you lost the money you sent to the scammer.

6. Robocalls

Sophisticated technology permits criminals to dial a large number of consumers from anywhere in the world and perpetrate many different scams upon their victims.

Robocalls that are NOT illegal

- Delayed school openings
- Dr. appointment reminders
- Flight cancellations
- Telemarketers (with your OK)
- Candidates running for office
- Charities requesting donations
- Debt collectors

Examples of robocall scams

- The caller tells you the warranty on your automobile or electronic device is expiring soon and payment must be made immediately to retain the coverage.
- The caller says “Can you hear me?” When you answer “Yes,” your reply is secretly recorded. The scammer calls back later and demands payment for goods or services that he claims you authorized. The recording of your “Yes” is used as proof that you agreed to pay for the goods or services.

7. Romance Scams

Many seniors seeking companionship use the internet as a means of trying to meet people. Scammers know that these individuals are often lonely and desperate, and try to exploit an individual's weakened state for money.

Romance scammers post fake profiles with attractive, alluring photos on dating sites in order to lure potential victims. These scammers, who often live in other countries, are skilled at what they do. They are very patient and give the appearance of being very caring as they "groom" their victims and gradually win their affection over time. Once they sense there's a connection, they tell the victim they need money for a sudden medical emergency or that they plan to visit the victim in the U.S. and need money for travel expenses and visas.

8a. **Internet Fraud**

Malware: Due to their unfamiliarity with internet technology, the elderly are easy prey for scammers as they browse the internet. Most older individuals, for example, would not hesitate to click on a pop-up window offering anti-virus software either free or at a low price. They believe they would be providing better protection for their computer.

In so doing, however, they are unknowingly allowing malware to be installed on their system which gives scammers unlimited access to their personal information. The individual is then vulnerable to identity theft and the loss of money.

8b. Internet Fraud

"*Phishing*" is the fraudulent practice of sending email messages that appear to originate from reputable entities such as government agencies, banks, credit card companies, or retail businesses in order to induce individuals to reveal personal information. Once individuals reveal personal information such as passwords, bank account numbers, credit card numbers, and social security numbers, the individual is vulnerable to identity theft and financial loss.

9. Elder Financial Abuse

Unlike other scams, financial abuse of the elderly is usually committed by someone the victim knows and trusts. It can be a family member, close friend, power of attorney, or caregiver. These individuals attempt to gain control of a senior's money, property, and credit cards, and display little concern for the individual's welfare in doing so. They often threaten to withhold food or necessary care in order to retain or gain control of the individual's assets.

Seniors who are physically disabled or cognitively impaired are at particular risk of being victims of this scam.

10. Charity Scams

Scammers know that older individuals willingly support charities in which they believe and that they are financially able to do so.

In order to entice potential donors, scammers set up fake charitable organizations with names that closely resemble those of legitimate charities. In so doing, they attempt to capitalize on the elderly's love of animals and their desire to help others who are less fortunate (e.g., hurricane and flood victims).

If you are asked to make a charitable contribution by cash, gift card, debit card, or wire transfer, don't do it. If the solicitor insists on sending someone to pick up your contribution, don't allow it. These are all signs that you're dealing with a scammer.

Charitable organizations in Illinois must register every year with the Attorney General's office. Before donating, you should confirm a charity's registration status at *illinoisattorneygeneral.gov* or 312-814-2595.

How to protect yourself from potential harm

1. Do not answer calls from unfamiliar numbers. Allow those calls to go into voice mail.
   - You can always retrieve a voice mail message at your convenience and return the call at another time if you wish.
   - By not answering such a call, your number is not classified as one that's answered and will not be sold to other criminals.
2. If you answer a call and are not comfortable with the tone of the conversation, hang up. You are not being rude by doing so.
3. If you receive an email and don't recognize the sender, delete the message. Do not click on any links or open any attachments.

(continued)

4. If you receive a threatening call regarding a past due bill or outstanding taxes, hang up. To confirm whether you actually have an outstanding balance, find the caller's legitimate telephone number from their website or from a previous statement, and contact the Customer Service Dept. Do not use contact information that was given to you by someone else.
5. Try to pay by check or credit card. Do not pay with cash, gift card, prepaid debit card, or wire transfer.
6. Consider using 2-factor authentication (2FA) to access your account(s).
7. Do not press any buttons on your phone to stop receiving Robocalls.

(continued)

8. Do not allow unvetted visitors to enter your residence for any reason (ruse burglaries).
9. Shred all paperwork that contains your personal information before discarding.
10. Make sure your computer's anti-virus software is current.
11. Exercise extreme caution when using your computer in public Wi-Fi environments (e.g., libraries, coffee shops, airports).
12. Be cautious of telephone calls, emails, and text messages with spelling and grammatical errors. These calls often originate from other countries.
13. If you are a victim of fraud, report it to the Federal Trade Commission at *reportfraud.ftc.gov* and your local police department.

Thank you for your interest and attention. I hope this information was helpful. Stay safe!

Questions and Comments?