PROTECT YOURSELF FROM COMMON CONSUMER SCAMS

Connecticut’s Senior Medicare Patrol (SMP) Program helps Medicare beneficiaries prevent, detect and report suspected health care fraud and abuse.

The Consumer Law Project for Elders is a project of Connecticut Legal Services, Inc.
THIS BOOKLET TELLS YOU:

☑️ What a scam is.................................................................2
☑️ Why seniors are frequent targets of scams.................2
☑️ Who the scammers are....................................................2
☑️ What the most common scams are.........................3-11
☑️ What you can do to prevent becoming a victim of a scam.................................................................12-13
☑️ Who to contact if you are a victim of a scam...........14
**WHAT IS A SCAM?**

Fraud, commonly known as a scam, is a crime that involves deceit, dishonesty, and/or swindling. People who commit scams are known as scammers or scam artists. Scammers try to get money or personal information from you, such as your Social Security number, bank account or credit card numbers. Scammers then use that personal information to purchase goods and services in your name or to take money from your accounts.

**WHY ARE SENIORS POPULAR TARGETS OF SCAMMERS?**

Several reasons have been given by experts.

Seniors often:

- Have money (pension, Social Security, savings) or assets (a home, stocks and bonds);
- Are home during the day and easy to contact;
- Tend to trust people, especially those who are polite;
- Are isolated and more willing to talk to strangers;
- Are more easily intimidated and less likely to take action or complain.

**WHO ARE THE SCAMMERS?**

**Strangers.** We all know to beware of strangers but people can still easily fall victim to them. Be very wary of any new person in your life, even a new romantic interest or friend, who wants to help with your finances or who asks for money or personal information.

**Family, friends and neighbors.** Sad as it is, people are often taken advantage of by their loved ones. Use good judgment when sharing your personal information with anyone, even your children.
COMMON SCAMS

Medicare Scams:
- You receive a Medicare Summary Notice and don’t recognize the doctor or service.

Some unscrupulous medical providers bill Medicare for services or equipment you never received.

ALWAYS CHECK YOUR MEDICARE SUMMARY NOTICE AND REPORT ANY ITEM YOU THINK IS INCORRECT.

- You receive a call from someone saying new Medicare cards are being issued. They ask you to confirm your Medicare number, Social Security number, date of birth or even say you must pay for the card to continue your benefits.

Medicare does not contact beneficiaries and ask them to update their information. Medicare issued new cards in 2018 and even then, it did not call people to confirm their personal information. If beneficiaries have a change in their personal information like a change of address, it is the responsibility of the beneficiary to update their information with Social Security.

Report Medicare fraud to:
Medicare: 1-800-633-4227, or
The Senior Medicare Patrol program: 1-800-994-9422

NEVER GIVE OUT YOUR MEDICARE NUMBER OR OTHER PERSONAL INFORMATION IF YOU GET AN UNSOLICITED CALL ABOUT MEDICARE.

Medical Identity Theft Scam:
- Medical identity theft occurs when a scammer gets your Medicare and other insurance information and uses it to receive health care. If any of the situations listed below happens to you, you could be a victim of medical identity theft.

You receive a bill for medical services you didn’t receive.

A debt collector contacts you about medical debt you don’t owe.

You try to make a legitimate insurance claim and Medicare says you have reached your limit on benefits when you know you haven’t.

You are denied coverage because your medical records show a condition you do not have.

PROTECT YOUR MEDICARE AND OTHER HEALTH INSURANCE CARDS. KEEP THEM IN A SAFE PLACE.
Gift Cards Scams

In many scams, people are being told to buy gift cards for payment. Victims are told to go to a store (like Walmart or CVS) and buy a gift card for a certain amount of money. Next you are asked to read off the numbers from the back of the gift card. With those numbers, the scammer can take the money from the gift card. Scammers like gift cards because they get immediate access to the victim’s money and the gift card cannot be traced.

**IF SOMEONE ASKS YOU TO PAY FOR SOMETHING WITH A GIFT CARD, IT IS A SCAM. GIFT CARDS ARE FOR GIFTS.**

Grandparent Scam: (phone)

You receive a phone call from someone who says he is a loved one (e.g. your grandchild) and is in trouble with the police, in the hospital, or stuck in another country, and needs money. He tells you not to tell his parents and to buy a gift card or wire money to a specific location. You do as you are told, but then you find out the call was not from your grandchild and a scammer now has your money.

**NEVER SEND ANY MONEY WITHOUT CHECKING WITH OTHERS TO BE SURE THIS CALL IS REAL.**

Fake Check Scam: (mail)

You receive a letter in the mail stating you have won money and enclosed is a large check. You are told to cash the check, keep a small amount of the money for yourself but send most of it back to the sender to cover taxes or processing fees. Because you are told you can keep some of the money, you trust the sender. You cash the check and send the money. In a few weeks, your bank tells you that the check bounced and you realize this was a scam. Your bank holds you responsible for paying it back the full amount of the bounced check.

**NEVER SEND MONEY TO ANYONE IN ORDER TO RECEIVE MONEY YOU HAVE “WON.”**
Prize Offers and Sweepstakes Scam: (telephone, mail, internet)
You are contacted by someone who offers you a “free” prize or says you have won something. The person then requests a fee to process your “winning entry,” or you are told you have to do something to obtain the prize - attend a sales presentation, buy something, or give out a credit card number. The scammer is trying to rope you in with these offers, hoping to get money or personal information from you.

NEVER GIVE MONEY TO ANYONE IN ORDER TO RECEIVE A PRIZE.

Foreign Country Scam (also known as Nigerian scam): (telephone, mail, internet)
You receive a call or email from someone who claims to be a foreign official, business person or the spouse of a former government official. He tells you that he needs to move money out of his country. He says he needs your help and offers you a huge reward. He then requests your bank account numbers, blank checks, cash or gift cards for the transaction. The scammer takes your money, rather than sending you some.

NEVER GIVE OUT PERSONAL INFORMATION TO SOMEONE YOU DO NOT KNOW.

Caller ID Spoofing Scam: (telephone, internet)
You receive a call from someone claiming to be a police officer investigating a fraud ring preying on elderly homeowners in your local area. You check your caller ID and it shows the call comes from your local police department, so you trust the caller. The caller may ask you to verify your name, Social Security number, bank account and credit or debit card numbers or other personal information. Because you trust the caller ID, you provide the information. You have been ‘spoofed.’ Spoofing is when a caller uses technology to cause a false name or phone number to appear on your caller ID. The caller ID may show the call is from the police, or Social Security Administration, IRS, FBI or any other entity that you likely trust. The spoofer now has your personal information and can obtain credit, loans or take money from your bank account.

DON'T ALWAYS BELIEVE THE PHONE NUMBER ON YOUR CALLER ID. NEVER GIVE OUT PERSONAL INFORMATION TO SOMEONE YOU DO NOT KNOW.
Phishing Scam: (text, email, internet)
You are emailed a document on letterhead of a legitimate company such as your bank, a government agency or a credit card company. The email tells you that the company is updating records, or that there has been a security breach and it needs to verify your information. You are asked to provide personal information, such as your Social Security number, bank account or credit card numbers. This is called “phishing” as the scammer is using fake letterhead to “fish” for personal information from people. The phisher then uses the personal information you provide to steal your money or buy things in your name.

NEVER GIVE OUT PERSONAL INFORMATION BY TEXT, EMAIL OR THE INTERNET TO SOMEONE YOU DO NOT KNOW.

Never pay someone with a gift card. Gift cards are for gifts.
Fake Charities Scam: (telephone, email)
You receive a call or email from someone who claims to be contacting you on behalf of a charity whose name may sound familiar to you but is really a phony charity. The caller asks for a donation by credit card or electronic bank withdrawal. If you ask to be sent something in writing, the caller refuses to send anything to you. If you provide the requested information, the scammer will use your credit card or take money from your bank account.

NEVER GIVE OUT PERSONAL INFORMATION BY TELEPHONE OR EMAIL UNLESS YOU MADE THE CONTACT YOURSELF.

Home Repair Scam: (in person)
Your door bell rings and at the door is someone who says he is a home repair contractor doing work in the neighborhood. He offers to look over your house to see if you need any work done. He then may offer to do a small job for a low fee as long as you let him do the work immediately. Once the work is done, he asks for a much higher fee. Or, he may tell you that you need more costly work done, such as a new roof or new windows that he will be happy to do, but he needs the full cost of the job upfront. Once paid, the scammer does a poor quality job or never shows up to do the job. In addition, if the repair allows the scammer to be inside your house, your valuables could be at risk.

ALWAYS CHECK THE LICENSE AND REPUTATION OF HOME REPAIR CONTRACTORS BEFORE HIRING THEM.
Home Rescue Scam: (telephone, mail, internet, in person)
You are contacted by a company claiming it has learned you are in financial difficulty and facing foreclosure. The company tells you that it can save you from foreclosure with a loan. You agree to the loan and sign a stack of papers without reading them. Without knowing, you sign the title of your home over to the scammer. You find out much later, when the scammer tries to evict you, that you no longer own the home and the money you have been paying each month on this so-called loan is rent.

NEVER GIVE OUT PERSONAL INFORMATION FOR A LOAN UNLESS YOU MADE THE CONTACT YOURSELF.
Social Security Number Scams: (phone, email)
You receive a call from someone who says she is from the Social Security Administration. She may say that your Social Security number has been blocked or suspended, or that Social Security wants to send you additional benefits, or protect you from a scam. Your caller ID may show the call is from the Social Security Administration. (See “Caller ID Spoofing Scam”). She asks you to confirm your full Social Security number or the last four digits. The scammer uses the personal information you provide to steal your money or buy things in your name.

Never give your Social Security number to anyone who calls or emails you asking for your Social Security number or other personal information.

Never give out personal information to someone you do not know.

Tech Support scam: (phone, computer)
You get a pop-up message on your computer screen, a voice message warning through your speakers or an urgent call from someone telling you that your computer has a virus. The screen or voice message may say they represent Microsoft or another large, reputable company. The message tells you not to shut down your computer and call a toll free number for assistance. Once you call, you are asked to give remote access to your computer so they can ‘fix’ the problem. They ask for your credit or debit card number to pay for the service they are going to provide. In reality, there is nothing wrong with your computer. You are being scammed. No legitimate tech support company would operate like this.

Ignore any urgent message or call from a supposed tech support company, never call the number on the screen.
IRS scams: (phone, email)

You are contacted by someone who claims to be from the Internal Revenue Service (IRS). Your caller ID may show the call is from the IRS (See “Caller ID Spoofing Scam”). The caller may give you a fake IRS identification badge number. You are told that you owe taxes and if you do not pay right away, you may be arrested and taken to court, have your driver’s license suspended or be deported. You are asked to give your bank account information, buy a gift card or wire money. Or you may be told you have a refund check coming, to trick you into providing personal information. Once you give the information they want, your money is stolen.

Do not respond to a phone call, voice message, or email from someone claiming to be from the IRS.
Romance scams: (email, internet)
Scammers use email, on-line dating sites and social media to meet potential victims. They learn things about you from your conversations then pretend to be the partner of your dreams. They will often express love for you in a relatively short period of time but give excuses as to why you can’t meet in person. Eventually, they will ask you to send money or gift cards or give them your bank or credit card account numbers. Once they have what they want, they take your money and disappear.

BEWARE OF ANY ONLINE LOVE INTEREST WHO ASKS YOU FOR MONEY, GIFT CARDS, BANK OR CREDIT ACCOUNT NUMBERS

Debt Relief scams: (phone, email, internet)
You are contacted by someone who says they can get rid of your debt or fix your credit. All you have to do is pay a fee upfront and all your debt and credit problems will go away. But these people do not have any intention of helping you. Instead, they want to take your money from you.

DO NOT BELIEVE ANYONE PROMISING TO GET RID OF YOUR DEBT OR FIX YOUR CREDIT.

Recovery Scams: (telephone, mail, internet, in person)
Beware! If you are a victim of any scam, you are likely to be contacted again by someone promising to get back any money you have lost to a scammer. This is another scam. Scammer’s sell “victim’s lists” to other scammers who contact those already scammed and offer to recover their money for a fee. Be careful not to lose more money in this common practice.
Beware! If you are a victim of any scam, you will likely to be contacted again by someone promising to get back any money you have lost to a scammer.

How can you avoid being scammed?

The goal in all of these scams is the same, to take your money from you or trick you into giving out personal information that is used to get credit cards, loans, health insurance or other valuable goods and services. Anyone can become a victim of a scam. Below are some tips to help you avoid becoming a victim:

- Never give personal information over the phone or by email or the internet unless you are familiar with the company/person or you made the contact yourself. Remember, Medicare, your bank and other legitimate companies will never ask for personal information over the phone, by email or the internet.

- Never buy a gift card to pay for something. Gift cards are for gifts.

- Never wire any money to someone unless you are sure it is someone you know.

- Don’t cash checks you receive in the mail unless you are certain you trust who the check is from.

- Don’t fall for “get rich quick” schemes. If something sounds too good to be true, it is probably a scam.

- Verify any phone, email or internet requests for money or personal information by contacting the person or company directly using a telephone number or email/web address you have looked up yourself and know to be genuine.

» continued
• Don’t respond to emails from people claiming to be from the government, financial institutions or companies asking for verification of personal information.

• Don’t click on links in any emails if the link is the only content in the text of the email, if the email is from someone you don’t know or if you have any question whether the sender really sent you the link.

• Don’t make charitable donations over the phone unless you initiate contact with a charity that you know.

• Beware of any salesperson or contractor who insists you give or send money to them immediately.

• Check out a company or individual with the Department of Consumer Protection (1-800-842-2649), Better Business Bureau (203-269-2700), or law enforcement agencies before you do business with them.

• Never pay in full upfront for any work that is to be done on your house.

• Be certain you are on a secure internet site before entering any personal information to purchase goods. Look for the little padlock sign in the address block that shows the site is secure.

• Consider first discussing any plan to sign a contract or purchase an expensive product with a trusted family member, friend or lawyer.

• If someone saying they are from Social Security calls or emails you requesting personal information, don’t respond. Instead, contact your local Social Security office or call 1-800-772-1213 (TTY 1-800-325-0778) to ask whether Social Security really needs any information from you. **The Social Security Administration will never call or email you to ask for your Social Security number.**

• Don’t ever give control of your computer, by phone or internet, to someone you do not know. If you get an urgent telephone message from someone who claims to be computer tech support and wants access to your computer, hang up. If a warning message appears on your computer screen telling you not to shut down your computer, shut down or unplug your computer for a few minutes. When you plug it in again, the message should be gone.

• To confirm whether you have been legitimately contacted by IRS, call the agency directly at 1-800-829-1040.
Who can I contact if I think I may be a victim of a scam?

To report Medicare scams contact:
CT's Senior Medicare Patrol (SMP) program: 1-800-994-9422
(operated at your local Area Agency on Aging)

Centers for Medicare & Medicaid Services
Call: 1-800-633-4227
TTY: 1-877-486-2048

HHS Office of Inspector General
Call: 1-800-447-8477
TTY: 1-800-377-4950
Online: https://oig.hhs.gov/fraud/report-fraud/
Mail: HHS Tips
P.O. Box 23489
Washington, DC 20026-3489

U.S. Senate Special Committee on Aging - Fraud Hotline (toll-free)
Call: 1-855-303-9470
Online: http://www.aging.senate.gov/fraud-hotline

To report or file complaints about non-Medicare fraud/scams contact:
Your local police department

The Consumer Law Project for Elders: 1-800-296-1467
(free legal assistance with consumer problems for CT residents ages 60 and over)

Connecticut Department of Consumer Protection: 1-800-842-2649
Better Business Bureau: 203-269-2700 or 860-740-4500
This publication was developed by Connecticut Legal Services, Inc. Consumer Law Project for Elders. This publication was supported by funding received by the Department of Rehabilitation Services, State Unit on Aging, in part by grant number 90MPPG004, from the U.S. Administration for Community Living, Department of Health and Human Services.

The Consumer Law Project for Elders provides free legal assistance to Connecticut residents 60 and over who have consumer problems. Call 1-800-296-1467.

Connecticut’s Senior Medicare Patrol Connecticut’s Senior Medicare Patrol (SMP) program helps Medicare beneficiaries prevent, detect and report suspected health care fraud and abuse. Call 1-800-994-9422 or visit https://portal.ct.gov/DORS-SMP

Revised: April 2019