SCAM JAM

AND SCAMS

You Have CHOICES
SMP
Empowering Seniors To Prevent Healthcare Fraud

The production of this booklet was supported in part by Grant No. 90MP0237 from the Administration on Aging, Administration for Community Living (ACL).

The Western CT Area Agency on Aging, Inc. (WCAAA) is a private, non-profit CT corporation that was designated as one of five CT Area Agencies on Aging by the CT State Legislature and Access Agency by the CT Department of Social Services.

Mission statement: The Western CT Area Agency on Aging, Inc. develops, manages and provides comprehensive services through person centered planning for seniors, caregivers, and individuals with disabilities in order to maintain their independence and quality of life".

Through a variety of federal, state and private funds, the WCAAA administers programs that provide direct services in community homes, provides grants and contracts to community non profit groups serving western area seniors to maintain community living and helps seniors with Medicare, Medicaid and other benefits' issues. Our Medicare fraud initiative is one of our center piece programs as we work with state and federal agencies to find and report fraud.

The Western CT Area Agency on Aging, Inc. (WCAAA) is pleased to distribute the "Scam Jam, Medicare Fraud and Abuse" and "Scam Jam Fraud and Scams" Booklets. The WCAAA Senior Medicare Patrol, (SMP) staff has spent many hours developing these two booklets for the different Fraud and Scams in Medicare on the hope that seniors and others will become highly aware of potential fraudsters. Please feel free to call the WCAAA with corrections and specific comments relative to these two booklets at 1-800-994-9422 (within 41 town area) or 203-757- 5449.

CONTENTS

WHAT IS SMP?

SMP is an acronym for the ***Senior Medicare Patrol*** Program. It started in 1997 and the U.S. Administration on Aging (AOA) is responsible for overseeing the SMP program which is part of the US Administration for Community Living (ACL).

Senior Medicare Patrols (SMPs) empower and assist Medicare beneficiaries, their families, and caregivers to prevent, detect, and report health care fraud, errors, and abuse through outreach, counseling, and education. SMPs are grant-funded projects of the federal U.S. Department of Health and Human Services (HHS), U.S. Administration for Community Living (ACL). Their work is in three main areas.

1) **Conduct Outreach and Education:** SMPs give presentations to groups, exhibit at events, and work one-on-one with Medicare beneficiaries. Since 1997 more than 30 million people have been reached during community education events, more than 6.5 million beneficiaries have been educated and served, and more than 46,000 volunteers have been active.
2) **Engage Volunteers.** Protecting older persons' health, finances, and medical identity while saving precious Medicare dollars is a cause that attracts civic-minded Americans. The SMP program engages over 5,200 volunteers nationally who collectively contribute more than 155,000 hours each year.
3) **Receive Beneficiary Complaints**. When Medicare beneficiaries, caregivers, and family members bring their complaints to the SMP, the SMP makes a determination about whether or not fraud, errors, or abuse is suspected. When fraud or abuse is suspected, they make referrals to the appropriate state and federal agencies for further investigation.

If you have questions or concerns about health care fraud, are interested in volunteering, or would like to schedule a free speaker, call the Western CT Area Agency on Aging at 203-757-5449 (1-800-994-9422)

The information and examples provided in this booklet about Medicare frauds and scams are **NOT MEANT TO ALARM OR FRIGHTEN YOU.** They are to **educate you** and help you identify signs of frauds and scams.

WHAT IS A FRAUD?

Fraud, commonly known as a scam; is a crime involving deception, dishonesty and / or cheating. People who commit fraud are known as scammers (Scammers, scam artists). The fraudsters try to get your money or personal information such as social security number, Medicare number, bank accounts or credit cards. Then scammers use your personal information to get goods or services on your behalf or to take money from your accounts.

FREQUENT VICTIMS OF FRAUD OR SCAMS?

Experts say that seniors are the most frequent victims of scams, and here are some reasons why.

Seniors often:

- Have money (pensions, collecting Social Security, savings) or properties (a house, stocks and bonds)
- Are in the house during the day and it is easy to contact them.
- Tend to trust people, especially people who are respectful.
- Are isolated and more willing to talk to unknown people.
- More easily intimidated and less likely to take action or complain.

WHO ARE THE SCAMMERS?

UNKNOWN PEOPLE: We all know that we should be careful with unknown people but it is easy to be a victim of them. Be very careful of any new person in your life, even if it is a new romantic couple, people who wants to help you with your finances, and stay away from those who ask for money or your information.

FAMILY, FRIENDS AND NEIGHBORS: While it is sad, loved ones are often the ones who take advantage. Use good judgment before

sharing your personal information with anyone, including your children.

SHOCKING NUMBERS!

Centers for Medicare and Medicaid Services (CMS), the federal agency that administers Medicare, reports that every year, millions of dollars are lost due to fraud, waste, abuse and improper payments. Below you will find recent statistics on National Healthcare fraud takedowns.

NATIONAL HEALTH CARE FRAUD TAKEDOWNS		
DATE	**# OF PEOPLE CHARGED**	**AMOUNT OF LOSS**
July 2010	94	$251 million
February 2011	111	$225 million
September 2011	91	$295 million
May 2012	107	$452 million
October 2012	91	$430 million
May 2013	89	$223 million
May 2014	90	$260 million
June 2015	243	$712 million
June 2016	275	~$800 million
TOTAL	Approx. 1,200	Over $3.5 billion

Based on the statistics, the amount money lost increases every year, along with the number of victims. It for this reason that SMP considers a priority reaching out to the community and helping them prevent being a target of health care fraud

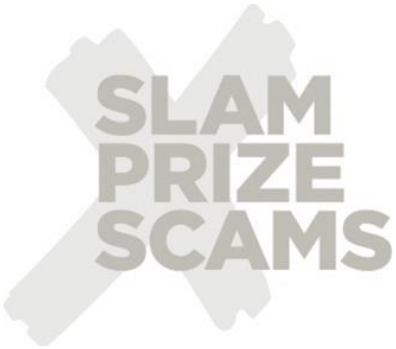
CRIMINAL AND CIVIL PENALTIES

Defrauding the Federal Government and its programs is illegal. Criminal and civil penalties for Medicare fraud reflect the serious harms associated with health care fraud and the need for aggressive and appropriate intervention. Providers and health care organizations involved in health care fraud risk exclusion from participating in all Federal health care programs and risk losing their professional licenses.


SCAMS
TARGET YOU
PROTECT YOURSELF

Prize Scams

You've just won $5000! or $5 million. or maybe it's a fabulous diamond ring, or luxury vacation? More likely, it's a PRIZE SCAM, and you'll find the prize isn't worth much. If you get a prize at all. Here's one way to think about it: **IF YOU HAVE TO PAY, IT IS NOT A PRIZE.**



Types of prize scams:

- **International Lottery Scams**: Typically, the letter will include a check. This is *a fake check scam*. Or a letter will say they're offering you a chance to enter a foreign lottery. The truth is that, even if your name was entered, it's illegal to play a foreign lottery.
- **Phone Scams**: Includes phone calls to let their targets know they won a "prize."
- **Using Money Transfer Services:** Scammers will contact you asking you for money so you can claim a "prize."

Signs of a Prize Scam:

Plenty of contests are run by reputable marketers and non-profits. But every day, people lose thousands of dollars to prize scams. Here are some signs you're dealing with a scam:

- **You have to pay:** Legitimate sweepstakes don't make you pay a fee or buy something to enter.
- **You have to wire money**: You may be told to wire money to an agent of "Lloyd's of London" or another well-known company — often in a foreign country — to "insure" delivery of the prize. Don't do it!
- **You have to deposit a check they've sent to you**: When you do, they'll ask you to wire a portion of the money back. The check will turn out to be a fake, and you will owe the bank any money you withdrew.

- **You're told they're from the government or another organization with a name that sounds official**: The Federal Trade Commission (FTC) doesn't oversee sweepstakes, and no federal government agency or legitimate sweepstakes company will contact you to ask for money so you can claim a prize.
- **Your "notice" was mailed by bulk rate**: It's not likely you've won a big prize if your notification was mailed by bulk rate. Other people got the same notice, too. Check the postmark on the envelope or postcard. Do you even remember entering? If not, odds are you didn't.
- **You have to attend a sales meeting to win**: If you agree to attend, you're likely to endure a high-pressure sales pitch. In fact, any pressure to "act now" before you miss out on a prize is a sign of a scam.
- **You get a call out of the blue, even though you're on the Do Not Call Registry:** Once you register your phone number for free at donotcall.gov, unwanted telemarketing calls should stop within 30 days. Unless the company falls under one of the exemptions, it shouldn't be calling: it's illegal.

Keep in mind that many questionable prize promotion companies don't stay in one place long enough to establish a track record, so if no complaints come up, it's no guarantee that the offer is real.

TELEMARKETING/PHONE SCAMS

Perhaps the most common scheme is when scammers use fake telemarketing calls to prey on older people. 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 buyers name is then shared with similar scammers.

- **Health survey:** In this scam, a caller will pretend to be from a marketing company that's collecting information for Medicare or from an independent research firm. Because there's no sales pitch, seniors might be more inclined to answer. But at the end of the call, the scammer will need to "verify" the senior's demographic data, which includes handing over a Medicare number.

- **"Can You Hear Me Now?"** This growing "can you hear me now?" phone scam may be the scariest scam yet because it can make you a victim if you say just one word, "YES".
  ***Your Plan*:** If you receive a phone call from someone asking, "can you hear me now?" **SIMPLY HANG UP**. You're a potential victim in the latest scam circulating around the Country. As the victim answers "yes," his or her reply is recorded. That enables the scammer, to use the recorded answer for signing up the victim for a product or service and then demand payment. Scammers also can use the recorded answer to confirm a purchase agreement if it is ever disputed. The best thing to do is "HANG UP".

- **Silent call:** Has this been happening to you? The phone rings, you pick it up, say "hello," but there's no one on the other line. According to the Financial Fraud Research Center, it's a new type of robot-call; an automated computer system making tens of thousands of calls to "build a list of humans to target for theft,". ***Your Plan*** If you haven't already done so, ask your phone company to put caller ID on your landline. Then simply screen your calls, and **don't pick up if the number is unfamiliar**.

TEXT MESSAGE PRIZE OFFERS

You get a text message that says you've won a gift card or other free prize. When you go to the website and enter your personal information, you'll also be asked to sign up for "trial offers" — offers that leave you with recurring monthly charges. Worse, the spammer could sell your information to identity thieves.

When you see a **spam text** offering a gift, gift card, or free service, report it to your carrier, then delete it. Don't reply or click on any links; often, they install **malware** on your device and take you to spoof sites that look real but are in business to steal your information.

INTERNET FRAUD

While using the internet is a great skill at any age, some may not be aware of all the scams on the internet. Examples include: e-mails from what looks like your bank asking for personal information. These e-mails often ask the recipient to click on a link provided to restore access to their online banking accounts; do not click on the link!

Your Plan: Call your bank first to see if there is an actual issue with your account. Remember always initiate the contact with any company or organization. Do not use the links or telephone numbers they provide for you. Please look up the telephone numbers yourself and you make the call. It may take a little time and effort but it will pay off in the end with less aggravation and heart ache.

Lastly, **click on a link only if you know it is safe to do so.**

DATING AND RELATIONSHIP SCAMS

You are looking for love or friendship. Aren't we all? Someone starts chatting with you through an online dating service and you enjoy the long chats with them and eventually become interested.

Over time you chat regularly and start to feel a strong bond. You may even start to fall head over heels for this person. But then right out of the blue they need some money – a looming personal crisis or a short-term lack of funds. You trust them obviously and you want to help. They will have a very convincing story to get you to send the money. Before long they ask for more – then more, and more, and more. Soon you've handed over all your savings. Or worse yet, you borrow money to bail them out.

Once they've taken all they can, your new love will disappear and your money will be gone. No one wants to think that they could fall

for an internet dating scam, and yet hundreds of people fall victim to such scams every single year.

SCAM ON CONNECTICUT ASISTANCE PROGRAMS

It is a "lead" generating business that populates senior citizen information lists for selling clients information other companies in exchange for a profit. The intent is to **misrepresent or "mask" their true purpose and confuse seniors**. Their postcard features a title in large, bold type: "**Medicare Savings Program**" and then goes on to present itself as an organization that will help seniors determine whether they qualify to have their Medicare Part B paid for by the state. Nowhere on the postcard does it say that they will "farm out" your information to other businesses and organizations. Again, this business is in the business of selling senior information lists to other companies for profit by way of misleading seniors.

Real Life Case Example:

A client brought a card that was mailed to her from Senior Supplemental Referral Service, P.O. Bo 4453, Boise, ID 83711-9977. It provides information on the "Medicare Savings Program," such as income and assets guidelines. It asked her to check off a box to affirm that she would like to apply. Subsequently, it asks for her name, age, phone number, spouse's name and age. ***At the bottom, it stated that it is not affiliated with or endorsed by any state or federal government or Medicare program***. We urge you to pay close attention to little words in any forms you receive, especially the ones you are not sure who is the sender.

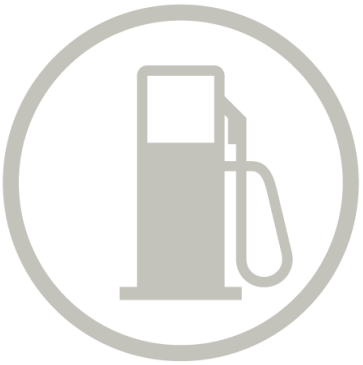
CHIP CARD SCAMS

Banks and Credit card companies have been issuing new **"chip cards."** This data is protected in an integrated circuit, rather than a magnetic strip and there's a dynamic code that resets after each use.

How to identify scammers: Scammers are sending you e-mails impersonating major credit card companies, using their logos etc. requesting personal and financial information. No Credit card company will email or call you to verify personal information it already has on file before mailing a new card.

CREDIT CARD SKIMMERS stealing personal info

Watch Out as you Pump Gas!



People are fueling their cars every day at the **gas pumps**, but ID thieves may be filling up on customers' financial information at the same time.

State regulators say they have found credit card skimming devices at gas station pumps that steal personal financial information, which can be passed on to hackers. The Department of Consumers Protection stated that many such devices have been found in CT in recent months throughout the state.

Identity thieves are now working to exploit the **gas pumps** by installing small processors that capture credit card numbers and, in some cases, PINs for debit cards. According to multiple reports, thieves are opening the doors of the **gas pumps** with a universal key that can be bought online. Police say people using credit or debit cards at the pump to buy gasoline should make sure **a seal covers a key hole that opens the pump**. If the seal has been tampered with, a device may have been installed to steal financial information.

CHECK SCAMS

Scammers know how to design phony checks to make them look legitimate. In fact, the Council of Better Business Bureaus just released a list of the most "risky" scams, based on how likely people are to be targeted, how likely to lose money, and how much money they lost.

Fake checks drive many types of scams – like those involving **phony prize wins, fake jobs, mystery shoppers, online classified ad sales, and others**. In a fake check scam, someone asks you to deposit a check – sometimes for several thousand dollars – and, when the funds seem to be available, wire the money to a third party. The scammers always have a good story, like: they're stuck out of the country, they need you to cover taxes or fees, you'll need to buy supplies, or something else. But when the bank discovers you've deposited a bad check, the scammer already has the money, and you're stuck paying the money back to the bank.

Don't deposit a check and wire money or send money back in any way. Banks must make funds from deposited checks available within days, but uncovering a fake check can take them weeks. If a check you deposit bounces – even after it seemed to clear – you're responsible for repaying the bank. Money orders and cashier's checks can also be counterfeit.

GIFT CARD SCAMS

This rip-off involves getting an unsolicited email from McDonald's, Subway or another popular restaurant or retailer offering a gift card if you click a link to activate it. The pitch looks legit, but it's a phishing scam, meaning the perpetrator is either trying to install malware on your computer or gather personal info by having you complete an online questionnaire.

Your Plan: Never click a link in an unsolicited email or divulge personal info, no matter how enticing the offer is. Do a Google search (such as "McDonald's gift card scam") and see if any warnings come up. In most cases, they will.

Furthermore, when you purchase a gift card, always make sure you request a receipt or the seller can skim off the card.

Real Life Case Example:

An individual purchased a gift card for a relative for $100. When the recipient went to use it, it was only worth $50.00. Always request a receipt in any gift card purchase to avoid being stolen.

FUNERAL AND CEMETERY SCAMS

Millions of Americans enter into contracts to prearrange their funerals and prepay some or all of the expenses involved, to ease the financial and emotional burdens on their families.

Laws in individual states regulate the industry, and various states have laws to help ensure that these advance payments are available when they are needed. However, protections vary widely from state to state, sometimes providing a window of opportunity for unscrupulous operators to overcharge expenses and list themselves as financial beneficiaries.

Tips for Avoiding Funeral and Cemetery Fraud:

- Be an informed consumer. Take time to call and shop around before making a purchase. Take a friend with you who may offer some perspective to help make difficult decisions. Funeral homes are required to provide detailed general price lists over the telephone or in writing.
- Educate yourself fully about caskets before you buy one, and understand that caskets are not required for direct cremations.
- Understand the difference between funeral home basic fees for professional services and any fees for additional services.
- Know that embalming rules are governed by state law and that embalming is not legally required for direct cremations.
- Carefully read all contracts and purchasing agreements before signing, and make certain that all of your requirements have been put in writing.
- Make sure you understand all contract cancellation and refund terms, as well as your portability options for transferring your contract to other funeral homes.

- Before you consider prepaying, make sure you are well informed. When you do make a plan for yourself, share your specific wishes with those close to you.
- *If a loved one passed away*: Ask a trusted family member to temporarily handle your financial responsibilities while you are grieving. Have that person follow up on any suspicious phone calls or emails. Be aware that while you are grieving, you may be more vulnerable to fraud tactics that play on your emotions.

THE GRANDPARENT SCAM

This scam uses one of the older adults' most reliable assets, their

hearts. Scammers will place call to an older person, when they pick up they will say, something along the lines of, "Hi Grandma, do you know who this is?" Once the identity is established the Fake grandchild will ask for money to solve some unexpected financial problem, overdue rent, payment for car repairs etc., to be paid via Western Union or Money Gram, which don't require identification to collect. At the same time. The scam artist will **beg** the grandparent *"Please don't tell my parents, they would kill me."*

THE IRS SCAM CALL

This scam is one of the most used.

Hackers are sending robot-calls to your phone, pretending to be the Internal Revenue Service (IRS). These callers might say, **"The IRS is filing a lawsuit against you."** Several people in Connecticut and around the country have been receiving these calls. They can certainly be very frightening if you don't know that this is a SCAM to get information from you.

REMEMBER: The **IRS does not call** people about back taxes, they will send you a notice by mail. **Hang up the Phone**, when the caller tells you they are from the IRS. **Do Not Respond!**

Dot click on any button on the number pad.

Two types of IRS scams

- **Fake notices that claim you owe money as a result of the Affordable Care Act ("Obamacare").** These are especially tricky, says the Federal Trade Commission, because their design mimics the real IRS notices.
- **Automated calls from the IRS claiming that you owe back taxes, and requesting you pay via gift card.** Sometimes these fake IRS calls are not automated, but rather a live person calling from a Washington, DC area code (202) using high pressure scare tactics to get your money (for example, saying the police are coming to arrest you for not paying your taxes). There are several red flags and tips to know whether you're dealing with the real IRS vs. a scammer:
    - The IRS never initiates contact with you via phone call, email, or through social media.
    - The IRS cannot threaten to have you arrested or deported for not paying.
    - You will never be asked to pay using a gift card, pre-paid debit card, or wire transfer; the IRS also never takes credit/debit card information over the phone.
    - If you owe the IRS back taxes, you will always have the opportunity to question or appeal the amount.

Did you know that you can report IRS SCAMS **ONLINE?** Go to the government web site for the Treasury Inspector General Administration (TIGTA) www.tigta.gov there will see a box on the Right-hand side.

You can send any suspect correspondence to phishing@irs.gov and let the FTC know. If you get a fake IRS call, hang up immediately and report it to the Treasury Inspector General for Tax Administration at *1-800-366-4484.*

VETERAN SCAM

Real Life Case Example

A Connecticut man has pleaded guilty to scamming more than a dozen military veterans out of more than $500,000 by promising to get them benefits that they never received.

Authorities say the scammer, a Vietnam veteran, told veterans that if they paid him he would help them get new or increased benefits from the Department of Veterans Affairs or the Social Security Administration. Instead, **the scammer kept the money for personal use.** Prosecutors say many of the veterans scammed suffer from service-related disabilities and chronic illnesses. The Scammer defrauded 15 veterans and one non-veteran out of more than **$525,000**.

If you are looking to apply for Veteran's benefits, we advise you to always contact legitimate centers for help, such as your local Area Agency on Aging at 800-994-9422, or the U.S. Department of Veterans Affairs at: 800-827-1000.

CON ARTISTS NETWORK.

"If you've been a victim of a fraud or scam, you're put on a so-called **sucker list**," "The lists are bought, sold, traded and stolen among scammers because they're perceived as potential gold mines. Scammers will usually target the victims with a 'recovery' or 'reload' scam. They pretend to be from a consumer group or law enforcement agency and trick you into thinking they'll help get your money back, of course, for a fee."

CANCER RIP-OFF

Real Life Data:

Last spring, in one of the biggest busts of its kind, the Federal Trade Commission (FTC) charged four national cancer charities *(the Cancer Fund of America, Cancer Support Services, the Children's Cancer Fund of America and the Breast Cancer Society)* with defrauding consumers of $187 million. At the other end of the cancer-scam spectrum, last August a reigning beauty queen (Miss Pennsylvania U.S. International) was arrested after allegedly claiming she had cancer and swindling tens of thousands of dollars from sympathetic supporters. She even shaved her head and staged "Bingo for Brandi" fundraisers, authorities say.

Your Plan: Before contributing to any charity, check out its rating on charitynavigator.org.

UNSCRUPULOUS FINANCIAL ADVISERS

Real Life Case Example:

Gideon Schein, a partner with Eddy & Schein In-Home Administrators for Seniors, says seniors have to be careful, even with trusted professionals. He cites an example of a client who had been paying $40,000 extra per month to a financial adviser who had known the client's father.

"My clients -- George, a retired math professor, and Elaine, a homemaker -- had their money with an institution for almost 20 years. I had been working for them for 2 years when their daughter called to ask me why her parents had spent so much money last year. I informed her that they did not. She then asked, 'What have I been

doing with $40,000 per month?'" Schein says. "I told her that I only got $20,000. Since the distributions were regular and sufficient, I had never asked to see a statement."

It turns out that their financial adviser had been taking $20,000 out of the distribution for himself. This had been going on for years. Their adviser was convicted of fraud and embezzlement, and the family was able to recover 70% of the money taken.

Most financial advisers have excellent credentials, experience and ethics abound, but it's always important to pay close attention to the money coming in and going out of your investment accounts.

BEWARE OF "STORM CHASERS" AND OTHER DOORSTEP CONTRACTORS

Storm Chasers typically follow the headlines and quickly move into regions hard hit by wind, flooding and the other ravages of weather. None the less, unethical contractors will visit neighborhoods to convince consumers and businesses that their property needs urgent repairs.

"Just because an individual has what looks like a registration number on their truck, business cards or other marketing material does not mean they are capable of doing the job safely or properly," says Connecticut Better Business Bureau spokesman Howard Schwartz. "They may be operating illegally, lack insurance or proper licensing and training."

Scam contractors attempt to **lure their victims with an appealingly low price, urge them to hand over a deposit and sign a contract on the spot, so that work may begin the following day**. Unfortunately, there are a number of possible unfortunate problems for victims.

Generally, after scamming consumers in one neighborhood or region, they will move on to find more victims in other states, cities and towns.

SCAMMERS TO PROMOTE HEALTH PRODUCTS

Scammers will do just about anything to rip you off. They will create fake websites, use fake endorsements from public figures, lie about the effectiveness of their products, and much more.

A number of shady companies selling "brain booster" pills are using these exact tactics to promote their products. Here's how:

They build spoofed websites that look like the news sites that we know and trust. The sites aren't real news sites and the endorsements featured on the sites, often from figures like Stephen Hawking, Anderson Cooper and others, are fake. Representatives from Hawking and Cooper have confirmed that neither has endorsed any "brain booster" products.

The spoofed news sites link you to the sales page for the product, which allows you to place an order with a credit or debit card. The scammers may claim that the pills are proven to work — that you'll experience an increase in concentration and memory recall by large percentages, but they lack evidence to support their claims. It's a scam.

The National Institutes of Health (NIH) advises that you talk to your doctor to get the facts about health products before purchasing.

If you already paid money to a scammer with a credit or debit card, you may still be able to get your money back.

- Call the card company immediately using the phone number found on your monthly statement.
- Alert them to the fraudulent charge right away.
- Ask if you are still eligible to get your money back.

- Ask if you should get a new card with a new number to prevent more fraudulent charges.

TECH SUPPORT SCAM

This just might be the biggest consumer scam in the U.S. right now. According to Microsoft, in 2015 an estimated 3.3 million people — many of them seniors — were victimized by a tech-support con, at a total cost of $1.5 billion. That's one American duped out of an average $454 nearly every 10 seconds.

Here's how the scam typically unfolds: You get an unsolicited call from someone claiming to be with Microsoft or Windows tech support, who says viruses have been detected on your computer. In order to protect your data, you are told to immediately call up a certain website and follow its instructions. A dummy screen may appear that shows viruses being detected and eliminated, but in reality, malware is being installed that allows the scammer to steal your usernames and passwords, hold your data for ransom or even use the webcam to spy on you.

Your Plan: Hang up the phone. "Neither Microsoft nor our partners make unsolicited phone calls," says Courtney Gregoire, senior attorney at the Microsoft Digital Crimes Unit. Also, don't click any links in unsolicited emails from "Microsoft" or in pop-up ads promising to speed up your computer. "And if you haven't downloaded Windows 10 or the latest version of OS X, do it," says William Woodworth with Best Buy's Geek Squad. "Each update is free and has lots of new security built in." Ditto for any other software programs you're running.

LOW COST TRIAL OFFERS, BEWARE

You've probably seen online ads with offers to let you try a product – or a service – for a very low cost, or even for free. Sometimes they're tempting: I mean, who doesn't want whiter teeth for a dollar plus shipping? Until the great deal turns into a rip-off. That's what the FTC says happened in a case it announced today.

The defendants sold tooth-whitening products under various names, and hired other companies to help them market the products. These affiliate marketers created online surveys, as well as ads for free or low-cost trials – all to drive people to the product's website. What happens next is so complicated that we created an infographic to explain it.

In short, once people ended up on the product's website, they filled in their info, put in their credit card number, and clicked "Complete Checkout." When people clicked this button they not only got the free trial of the one product, but were actually agreeing to monthly shipments of the product at a cost of $94.31 each month.

Next, another screen came up and people were asked to click "Complete Checkout" again. But the second screen wasn't a confirmation screen for the trial of the product. Instead, by clicking this button people were actually agreeing to monthly shipments of a second product. So, what started as a $1.03 (plus shipping) trial of **one** product wound up being an unexpected **two** products at a very unexpected $94.31 each – for a total monthly charge of $188.96 plus shipping.

Trial offers can be tricky – and there is often a catch. – and there is often a catch. If you're tempted, do some research first, and read the terms and conditions of the offer very closely.

EQUIFAX ISN'T CALLING!

Ring, ring. "This is Equifax calling to verify your account information." Stop. Don't tell them anything. They're not from Equifax. It's a scam. Equifax will not call you out of the blue. That's just one scam you might see after Equifax's recent data breach. Other calls might try to trick you into giving your personal information. Here are some tips for recognizing and preventing phone scams and imposter scams:

- **Don't give personal information.** Don't provide any personal or financial information unless you've initiated the call and it's to a phone number you know is correct.
- **Don't trust caller ID.** Scammers can spoof their numbers so it looks like they are calling from a particular company, even when they're not.
- **If you get a robo call, hang up.** Don't press 1 to speak to a live operator or any other key to take your number off the list. If you respond by pressing any number, it will probably just lead to more robo calls.

If you've already received a call that you think is fake, report it to the FTC.

If you gave your personal information to an imposter, it's time to change any compromised passwords, account numbers or security questions. And if you're concerned about identity theft, visit IdentityTheft.gov to learn how you can protect yourself.

For more information about the Equifax breach, visit Equifax's website, www.equifaxsecurity2017.com or contact their call center at 866-447-7559.

Jury Duty Scam

It has been reported by several CT Police Department Officials that scammers are calling claiming to be a member of law enforcement, whether it's the local police, the sheriff's department or the U.S. Marshals Service. The caller typically tells the victim that they have failed to appear for jury duty, failed to answer a court summons or have an active warrant for their arrest, which they may tell you was just signed by a judge.

The caller ID may show phone numbers for a courthouse or law enforcement agency, and the caller may cite names of actual police officers, court officials, judges or town officials. The caller will tell the victim that they can pay a fine to avoid arrest. They will request this payment through prepaid cards, gift cards or wire transfer. The caller may even ask to the victim to confirm their identity by soliciting personal information, including your name, birth date, Social Security number and other ID theft-worthy details.
According to many Local Police Departments, "The jury duty scam remains one of the most successful intimidation/imposter schemes, "scammers can not only get a quick payoff but also enough personal details for future identity theft."
Police recommend that people receiving this call **HANG UP** without providing any information.

TAKING ADVANTAGE OF DEMENTIA

Real Life Case Experience

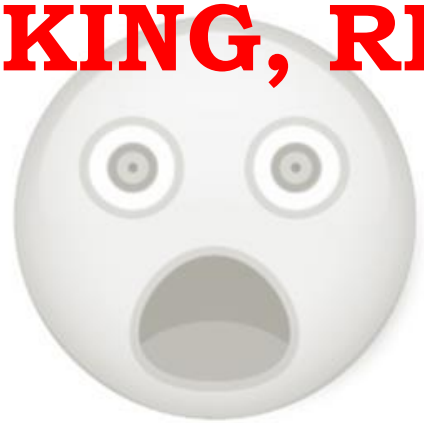
People with Dementia are also at risk of scammers. An 82-year-old former youth pastor and retired social worker for the city of San Francisco has always been outgoing and trusting. "As dementia has taken more hold, it has exposed more trust."

Thieves made small, automatic withdrawals from the client's personal checking account for about a year, stealing around $2,000 in withdrawals that the bank couldn't trace.

DO NOT GIVE OUT PERSONAL INFORMATION, CREDIT CARD OR BANK ACCOUNT NUMBERS

…

SHOCKING, RIGHT?



TIPS TO PREVENT FRAUD AND SCAMS

HOW CAN YOU PREVENT THIS FROM HAPPENING TO YOU?

The purpose of all scams is the same: To obtain your personal information and to have access to your credit cards, bank accounts or investments, and / or health insurance.

Therefore, it is important that you

PROTECT yourself from fraud, abuse and scams.

DETECT: Learn to detect potential fraud, abuse or scams.

REPORT: If you suspect that you have been a target of fraud, abuse or scams, always report it.

USEFUL TIPS:

Although anyone can be a victim of scams, here are some tips to avoid being one.

- Never provide your personal information by phone, email or online, unless you know the company or person, or it was you who initiated the contact. **REMEMBER**, Medicare, your bank, IRS or other legitimate companies will never ask for your personal information by phone, email or online.
- Treat your Medicare, Medicaid and Social Security numbers like a credit card number. Never give these numbers to a stranger. **REMEMBER**, Medicare doesn't call or visit to sell you anything
- Don't carry your Medicare or Medicaid card unless you will need it. Only take it to doctor's appointments, visits to your hospital or clinic, or trips to the pharmacy.
- Record doctor visits.
- Save Medicare Summary Notices and Part D Explanation of Benefits.
- Always review your Medicare Summary Notice (MSN) and Part D Explanation of Benefits (EOB) for mistakes. And compare

your MSN and EOB to your personal health care journal and prescription drug receipts to make sure they are correct.

- **Look for three things on your healthcare billing statement:**
  1. Charges for something you didn't get.
  2. Billing for the same thing twice.
  3. Services that were not ordered by your doctor.
- **Shred** the documents when they are no longer useful.
- **Never send money** to anyone unless you are sure that it is someone you know.
- Do not deposit a check you received in the mail unless you are sure you trust who the sender is.
- Do not fall into the trap of "Be Rich Faster." **if something sounds too good** to be true, it is probably a scam.
- Always check any phone number, email address or website asking for money or your personal information.
- **Do not respond** to emails from financial institutions or companies that ask you to verify your personal information.
- **Do not click on any internet link** that you receive by email, especially if it comes from someone you do not know.
- **Do not make charitable donations by phone**. Ask the caller to send you a printed form to make your donation.
- **Do not pay** any vendor or contractor who insists that you give or send money immediately prior to receive or initiate services.
- Make sure you are on a legitimate internet site before entering your personal information when shopping. **Look for the lock symbol** in the address block showing that the site is secure.
- Before signing a contract or buying an expensive product, consider talking it over with a relative, friend or lawyer you trust.
- **If you have questions** about information on your Medicare Summary Notice or Part D Explanation of Benefits, call your provider or plan first.

- Before doing business with a company or individual, always investigate them with the Department of CT Consumer Protection: 1800-842-2649, with the Better Business Bureau 203-269-2700.
- **REMEMBER: SMP is always here to assist you, you can reach us by Calling CHOICES at Western CT Area Agency on Aging at 203-757-5449.**

INFORMATION SOURCES:

- Federal Trade Commission
- Better Business Bureau
- Consumer Specialist, Federal Trade Commission
- Senior Medicare Patrol Navigator
- The Consumer Law Project for Elders
- Centers for Medicare and Medicaid Services (CMS)
- Office of Inspector General: US. Department of Health and Human Services.

WHO TO CONTACT IF YOU SUSPECT YOU ARE A VICTIM OF HEALTHCARE FRAUD OR SCAM?

CT's Senior Medicare Patrol Program: 1800-994-9422 IS PART OF the CHOICES program in your local Agency on Aging – Waterbury: 203-757-5449 EXT 160 OR 1800-994-9422).

- Centers for Medicare & Medicaid Services:
  Phone Number: 1800-633-4227
  TTY: 1-800-486-2048
  Postal Address: Medicare Beneficiary Contact Center
  P.O. Box 39
  Lawrence, KS 66044
- HHS Office of Inspector General
  Phone Number: 1-800-477-8477
  TTY: 1800-377-49-50
  Website: https://forms.oig.hhs.gov/hotlineoperations/report-fraud-form.aspx
  Postal Address: HHS Tips Hotline
  P.O. Box 23489
  Washington, DC 20026-3489
- U.S. Senate Special Committee on Aging-Fraud Hotline
  Toll Free Number to report fraud: 1-855-303-9470
  Website: www.aging.senate.gov/fraud-hotline
- Connecticut Attorney General's Office
  Phone number: 860-808-5354
  Fax: 860-808-5033
  E-mail Address: ag.fraud@ct.gov
  Postal Address: Office of the Attorney General
  Antitrust and Government Program Fraud Department
  Fraud Complaint
  P.O. Box 120
  Hartford, CT 06141-0120

FOR ALL OTHER TYPES OF FRAUD OR SCAMS CONTACT…

- Local Police Department.
- The Consumer Law Project for Elders: 1800-296-1467.
- CT Department of Consumer Protection: 1800-842-2649.
- Better Business Bureau: 203-269-2700.
- **Federal Trade Commission: 1-877-FTC-HELP (1-877-382-4357).**
- Division of Consumer & Business Education, FTC

NOTES

October 2017

Western CT Area Agency on Aging