PREVENTING AND RECOVERING FROM SCAMS, FRAUD, AND IDENTITY THEFT FOR SENIORS AND THE DISABLED

Matthew M. Santelli
Education and Outreach Specialist
Pierce County Aging and Disabilities
Resource Center

A Summary Of Today's Presentation

1. Upcoming public events of interest
2. Planning safety at home
3. Taking a quiz together to test our skills
4. Knowing the targets of scams / fraud / identity theft
5. The importance of protecting personal information
6. Understanding opportunity / availability / response
7. Common methods that scammers use
8. Sweetheart scams explained
9. Understanding and avoiding scams / fraud online
10. How to recover if you are a victim

Planning Safety At Home

1. Lighting around entryways all around the house
2. Locked doors and windows
3. Peephole in your door (no good unless you use it)
4. Ring doorbell with monitored camera and microphone
5. Burglar and smoke and carbon monoxide alarms
6. 676 motor vehicles stolen in Pierce County during June 2023 – many more have windows smashed out or doors broken open
7. Lock car doors and close windows
8. Leave nothing of value in your car including the garage door opener!
9. Never leave the motor running without you locked in the car!
10. Do not step out of your car at the scene of an accident unless you must do so for safety! Call 911 then call friends or family members

Let’s Quiz Ourselves To Test Our Ability To Avoid Scams/Fraud/Identity Theft

Take the following quiz to determine your risk of becoming an identity theft victim. Answer each question as follows:

1= I never do this

2= I rarely (every once in a while) do this

3= I do this about 50 percent of the time

4= I usually (almost always) do this

5= I always do this

The higher your score, the fewer opportunities you are providing for identity thieves to steal key pieces of identifying information or for evidence of identity theft to go unnoticed.

Checking For Evidence Of Scams/Fraud/Identity Theft

_____ 1. I check my credit report from each of the three major credit bureaus (Equifax, Experian, and Trans Union) annually to look for errors and evidence of identity theft.

_____ 2. I review bank and/or brokerage account statements when they arrive to reconcile the balance and to check for unusual transactions.

_____ 3. I save credit card receipts and check them against statements received from creditors. I do not leave them in shopping bags, where they can get lost or stolen.

_____ 4. I know the approximate billing cycle for all of my credit cards and utility bills (e.g., cell phone) and call creditors immediately if bills are not received within a week of the due date.

Destroying Sensitive Personal Information

_____ 5. I use a crosscut shredder, fireplace, or woodstove to destroy pre-approved credit card offers, bank or brokerage statements, old pay stubs and tax records, credit card receipts, and other “sensitive” documents.

_____ 6. I destroy (shred or burn) everything that contains information of interest to identity thieves including utility bills (which could be used to obtain a credit report), personal correspondence (which could be used to corroborate my identity), cancelled checks, expired credit cards, etc.

Limiting Access To Sensitive Personal Information

_____ 7. I avoid giving out my Social Security number or bank account numbers to unsolicited callers or orally (e.g., in a store) where others may be listening.

_____ 8. I have a post office box or a locked mailbox for incoming mail (especially checks and bills).

_____ 9. I place outgoing mail in a secured collection box along the road or at the post office- NOT in an unsecured home mailbox or rural route mailbox along the highway.

_____10. I have my mail held when I am away or picked up by a trusted friend, neighbor, or family member.

_____11. I question how personal information will be used before revealing it to anyone and try to “just say no,” where possible or ask to use another type of identifier.

_____12. I am cautious about not leaving personal information lying around my home, especially if it would be accessible to a roommate, babysitter, cleaning service, home contractor, etc. who has access to my home when I am not there.

Limiting Access To Sensitive Personal Information (cont'd)

_____ 13. I avoid carrying my Social Security card in my wallet as well as any type of identification card with my Social Security number (or my spouse's social security number) on it.

_____ 14. I avoid printing my driver's license or Social Security number on personal checks.

_____ 15. I limit the amount of personal information "out there" by not completing Internet "profiles" for rebates and contests and being cautious with online resume posting, electronic mailing lists, secured sites for online purchases, listings in Who's Who Guides, and other public data sources.

_____ 16. I limit the number of credit cards and other identification information that I routinely carry around in my wallet or purse and I do not routinely carry around my checkbook.

_____ 17. I am aware of who has access to my personal information at work and/or places I do business with (e.g., utility companies, medical providers) and have taken steps to question or limit unauthorized access, where needed.

_____ 18. I cross out my credit card number or bank account number with a magic marker on receipts for travel or other expenses that I submit to an employer, charitable or professional organization, or other entity for expense reimbursement or for documentation of any type (e.g., taxes, product rebates).

Limiting Access To Sensitive Personal Information (cont'd)

_____ 19. I am careful about completing postcards (e.g., for product warranties, contests, etc.) and place them in envelopes if they contain sensitive information.

_____ 20. I practice "general security consciousness" by not leaving my wallet or purse unattended, even for a few minutes (e.g., at dances or on supermarket carts), zipping my purse shut, buttoning my back wallet pocket, and putting house lights on timers when I'm away. Also, using secure door locks, leaving questionable "sensitive" information spaces blank on applications, storing important papers (e.g., car title) in a safe deposit box, not using bank deposit slips or paycheck stubs for shopping lists, and keeping a list of credit card account numbers and contact information to report a loss quickly.

What Your Quiz Score Means:

80 to 100 Points- You have demonstrated a higher than average awareness of the risks associated with identity theft. Congratulations. Do not let your guard down! Identity thieves are always looking for another victim.

50 to 79 Points- You have indicated some weaknesses in your security consciousness, which increases your odds of becoming the victim of identity theft, especially if you have good credit. Pay particular attention to the quiz questions that you answered with a "1" or "2."

0 to 49 Points- You are at high risk for identity theft. Start shredding sensitive personal and financial documents immediately and pay particular attention to quiz questions that you answered "1" or "2".

Who Are The Main Targets Of Scams And Fraud?

The fifty-years-and-over age group make up *one-half* of all fraud victims overall and make up *one-third* of all telemarketing fraud victims.

The twenty-five-years-and-under age group are the *next* largest group of all fraud victims overall.

Social media like Instagram, Facebook, and Snapchat have made young people easy targets for scammers.

Important Things To Remember About Scams/Fraud/Identity Theft

- Any of us could fall victim to a scam, age alone does not make us vulnerable.
- People who are more isolated are more at risk.
- Victims may worry that revealing their experience will lead to losing their independence or financial autonomy.
- Scam victims are more likely to be targeted for future scams.
- Scammers tend to force people into make ‘split second’ decisions, not allowing them to consider what is happening.
- Scammers may have become part of daily life of the victim.

How Can Scams And Fraud Result In Identity Theft?

Theft of your personal information by deception (such as names, dates of birth, social security numbers, and bank account numbers) can allow crooks to steal your identity

Breaches/hacking of your online user names, passwords, and security verifications can allow crooks access to your data stored on computers

Learn to protect your personal information!

Why Are Scams/fraud Frequently Targeted At Seniors And The Disabled?

- Crooks who perpetrate scams and fraud often seek to exploit current events, such as the COVID-19 outbreak. They do this by selling phony tests, treatments, or cures; by claiming that fees must be paid for tests or vaccines, by promoting fraudulent charitable causes, and by financially defrauding those who are worried about the outbreak.
- Crooks understand that seniors and the disabled are easy to target because of their *opportunity*, *availability,* and *response.*

How Does *Opportunity*, *Availability*, And *Response* Make Seniors And The Disabled Easy Targets?

- **Opportunity**: Crooks know that seniors and the disabled have reliable sources of income such as monthly Social Security payments, pension payments, and IRS tax refunds. These payments give the crooks the financial *opportunity* to commit scams and fraud.

- The crooks do not care if your income or savings are high or low! They still will target you!

- The crooks review public government pages such as real estate records and recorded documents to learn more about you.

How Does *Opportunity*, *Availability*, And *Response* Make Seniors And The Disabled Easy Targets? (cont'd)

- **Availability**: Crooks know that most seniors and disabled adults are no longer working, so they are targeted at home. Staying at home gives the crooks the *availability* to contact seniors and disabled adults through phone calls and text messages, through US mail, through email, and through front door visits to their homes.
- **Response**: Crooks know that seniors and the disabled are typically courteous, polite, thoughtful, and willing to provide a generous *response* to those who make contact with them.

How Do Crooks Approach Victims To Commit Scams And Fraud?

- Victims are approached through the US Mail, by phone, at the front door, in public places, and over computer websites/email.
- The more often that we engage crooks when they approach us, the more likely we are to become victims.
- Learn how to say no without asking permission!
- It is okay to speak rudely to a crook! Do not apologize to them!
- Stop before acting out of fear, worry, or urgency and then call a trusted friend or neighbor for guidance.

Some Recent Examples Of Scams And Fraud

- Money mule scams can involve organized crime networks. In these scams you may receive “winnings” or a “settlement” sent as cash or a money order. You are then instructed to call a number to confirm receipt, then told to make a deposit and then wire transfer it to another account.

- The old familiar “grandchild in trouble” phone call scam has now been adapted to fit the COVID-19 outbreak. In this version of the scam, a crook will call a senior, pretending to be a grandchild or other young relative. The crook will then say to the senior, “It is me and I need help from grandma/grandpa, I am sick in a hospital with COVID-19 and I cannot be treated or given medication unless you send money to me”. Of course, there is no sick grandchild or young relative, and the crook is simply hoping that grandma/grandpa will be frightened and will then wire money or give out credit card info on the phone.

More Examples Of Recent Scams And Fraud (cont'd)

- Unsolicited phone, text, email, or US Mail requests for charitable donations to fraudulent charitable organizations claiming to be providing help to people or even animals in need. Charitable organizations that are properly operating in the State of Washington can be verified through the Secretary of State's office at **(360) 725-0378** or **www.sos.wa.gov**.
- Sweetheart scams often occur on the computer through popup malware, email contacts, or through online dating sites. Scammers often portray themselves as overseas royalty, US military personnel, oil field workers, or flight attendants.
- Victims become convinced that the scammers truly love them.

Sweetheart Scam Characteristics

1. Build rapport (they discuss things in common)
2. Gain trust (victim and scammer share their secrets)
3. Build relationship (victim becomes the ideal partner and sees the scammer as the same)
4. Establish plans for the future (victim and scammer make plans to be together)
5. Request financial assistance to make future plans happen (usually in context of a complex situation that requires victim to provide money to the scammer to resolve a legal issue so that the scammer can travel to meet the victim)

Vaccine Scams That The FBI Have Warned About Include:

- Ads offering early access to the vaccine for a fee.
- Requests for people to pay to put their names on a vaccine waitlist.
- Offers to have doses of the vaccine shipped to your house.
- Emails or phone calls or text messages from someone claiming to be at a vaccine center or medical office or insurance company or government office asking for personal and medical details to verify eligibility to obtain the vaccine.

There Are No Fees Needed For Anyone To Receive The COVID-19 Vaccine!

- By government mandate, all public and private health insurance plans MUST OFFER the COVID-19 vaccine with no out-of-pocket fees required from the recipient
- Uninsured individuals also will be offered the COVID-19 vaccine with no out-of-pocket fees required

Home testing kits for COVID-19 are free at local libraries and billable to Medicare Part B at local pharmacies!
Paxlovid treatment is available!

A Word About WA Cares To Avoid Scams/Fraud

- WA Cares is another term used to describe the Washington Long-Term Care Trust Act.
- WA Cares is a first-in-the-nation program that ensures working Washingtonians can access affordable long-term care coverage.
- Workers began contributing to the WA Cares Fund on July 1, 2023.
- Workers contribute 0.58% of each paycheck to the WA Cares Fund.
- Benefits totaling $36,500 per person will NOT BE AVAILABLE until July 1, 2026, at the earliest, and then only for active workers who paid into the WA Cares Fund for three consecutive years.
- People who are not actively working are NOT ELIGIBLE for WA Cares benefits, including current retired seniors and current disabled adults.

DO NOT FALL PREY TO SCAMS/FRAUD ABOUT WA CARES! THERE ARE NO SIGNUPS OR BUY-INS FOR THIS PROGRAM! THE PAYROLL DEDUCTION FOR WORKERS IS A STATE REQUIREMENT OF THEIR EMPLOYERS!

Identifying Risks That We Encounter Online

- Electronic transactions and information gathering are now the norm and will only become more sophisticated in the future, due to the development of A.I. (artificial intelligence).
- Any internet connection leaves the user at risk of scams and fraud, whether on a home computer, tablet, laptop, or phone.
- Spoofing, spamming, cloning, account hacking, redirecting, spyware, malware, keystroke tracking, and camera hijacking are all methods to attack devices that we use.
- Phishing, fake identities, fake websites, cookies, fraudulent links, malicious pop-ups, fake update requests, online extortion, are all methods to fool users into giving up personal information.

Let's Define These Terms To Understand Them

Spoofing: A type of scam in which a criminal disguises an email address, display name, phone number, text message, or website URL to convince a target that they are interacting with a known, trusted source. Spoofing often involves changing just one letter, number, or symbol of the communication so that it looks valid at a quick glance. For example, you could receive an email that appears to be from Netflix using the fake domain name "netffix.com."

Spam: A term that describes unwanted, unsolicited communications, including email.

Cloning: Copying your phone number to another phone. The scammer then uses your mobile phone number as the key to your most important financial accounts. Text messages are often used by banks, businesses and payment services to verify your identity when you request updates to your account.

Account hacking: When a scammer takes control of your email or social media account or website. The scammer then sends messages that look like they are yours.

Redirecting: When a website that you click on sends you to another website, usually to sell you a product or service or to convince you to provide personal information.

Spyware: A type of malware that is installed on your device without your knowledge or permission, covertly gathering intel about you.

Let’s Define These Terms (cont’d)

Malware: Malicious software that harms or exploits devices, data, or networks.
Keyloggers: A particularly insidious type of spyware that can record and steal consecutive keystrokes (and much more) that the user enters on a device.
Cookies: Computer cookies are small files used by web servers to save browsing information, allowing websites to remember your device, browser preferences, and associated online activity.
Camera hijacking: A malware which allows a hacker to gain access to a webcam, allowing them to turn it on, then watch and record everything that goes on, all without the victim realizing.
Phishing: The fraudulent practice of sending emails or other messages, purporting to be from reputable companies, in order to induce you to reveal personal information, passwords and credit card numbers.
Fake identities: These result from an account hack or spoofing a phone number or email. Facebook Messenger accounts have shown fake identities recently when Taylor Swift toured the country, by offering concert tickets for sale.

Let's Define These Terms (cont'd)

Fraudulent links: These lead to phony websites and / or can launch malware onto your computer.
Malicious popups: Malicious pages that take over your screen view to give fake warnings or prize announcements.
Fake update requests: Official-looking popups that tell you to update your computer programs like Adobe Acrobat or Norton Antivirus.
Online extortion: Scammer threats to release information or photos that will embarrass the victim so that the victim will pay the scammer money. These threats have resulted in the suicide of several young adults who had sent photos of themselves to scammers who were pretending to be online girlfriends or boyfriends.

Safety Tips To Avoid Online Scams And Fraud

(More info at https://seniorsafetyadvice.com/security/)

1. Make Your Passwords Strong To Decrease The Chances They Can Be Cracked
2. Avoid Entering Personal Information On Unfamiliar Websites
3. Always Have A Secure Internet Connection
4. Install An Antivirus And Malware Program On Your Computer
5. Avoid Clicking On Links In Your Emails
6. Be Careful About What You Download And Where You Download It From
7. Be Careful About Purchasing Items Through A Social Media Site
8. Be Careful About What You Say Online
9. Be Extra Cautious About Who You “Meet” Online
10. Designate One Person You Trust With The “Key” To Your Data

How To Recover If You Are A Victim

- Make sure to maintain a list of all your open bank, credit, and retail accounts in a safe
- place at home.
- If a fraudulent charge is made with one of these accounts, make a report to the bank/credit card company/retail outlet as soon as possible. Keep notes about your conversations (who/what/when).
- Use the listed phone numbers on the cards to contact them and keep notes – do not share information on a call from someone claiming to be from the bank/credit card company/retail outlet because it might be a scam!
- Call local police non-emergency number to make a report and obtain a case number, which you might need to provide to the bank/credit card company/retail outlet, so no fraudulent charges are billed back to you.
- Check your credit reports for free: https://www.annualcreditreport.com
- Shred your documents that have identifying information on them.
- Hire a reputable computer or phone repair business to service computer / phone.
- Learn from your experience to avoid being a victim in the future!

Additional Resources:

- For more information about preventing and recovering from all scams and fraud, contact Pierce County Aging and Disabilities Resource Center (ADRC) at **(253) 798-4600**, or visit: **www.pierceadrc.org** or **www.ftc.gov**.
- For COVID-19 questions and vaccine clinics, contact Pierce County Health Department at **(253) 649-1412** or your physician or your pharmacist or visit: **https://coronavirus.wa.gov/ or www.tpchd.org.**
- To verify charitable organizations operating in the State of Washington, contact the Secretary of State's office at **(360) 725-0378**, or visit: **www.sos.wa.gov**.
- For more information about the Washington State Long-Term Care Trust Act (WA Cares) please visit: **www.wacaresfund.wa.gov**.
- For more information about programs, services, and public events for seniors and disabled adults in Pierce County, contact Pierce County ADRC at **(253) 798-4600** or visit: **www.pierceadrc.org**.