

# Safe & Secure Seniors

Elder Abuse in the Digital Age

Southwest Virginia Legal Aid Conference



Presented by: Marnie Stewart

President, Senior Housing Crime Prevention Foundation



Senior Housing Crime  
Prevention Foundation

# Senior Housing Crime Prevention Foundation

- Founded in 2000
- The SHCP Foundation exists to promote safety and security in senior living facilities: nursing homes, HUD communities, state Veterans homes, assisted living communities and independent living communities – and provide residents with an enhanced quality of life.
- We are funded by the banking industry's interest in community reinvestment



# What is Elder Financial Abuse?



- Illegal or improper use of an older adult's money or property.
- Significant and growing problem, affecting millions of older adults worldwide
- The Digital Age has created new opportunities for perpetrators to exploit older adults financially.

# Increased Opportunity for Fraud

## By 2030

- All baby boomers will be older than 65, and the Census Bureau projects that will grow the size of the older population so much **that 1 in 5 people in the U.S. will be retirement age.**

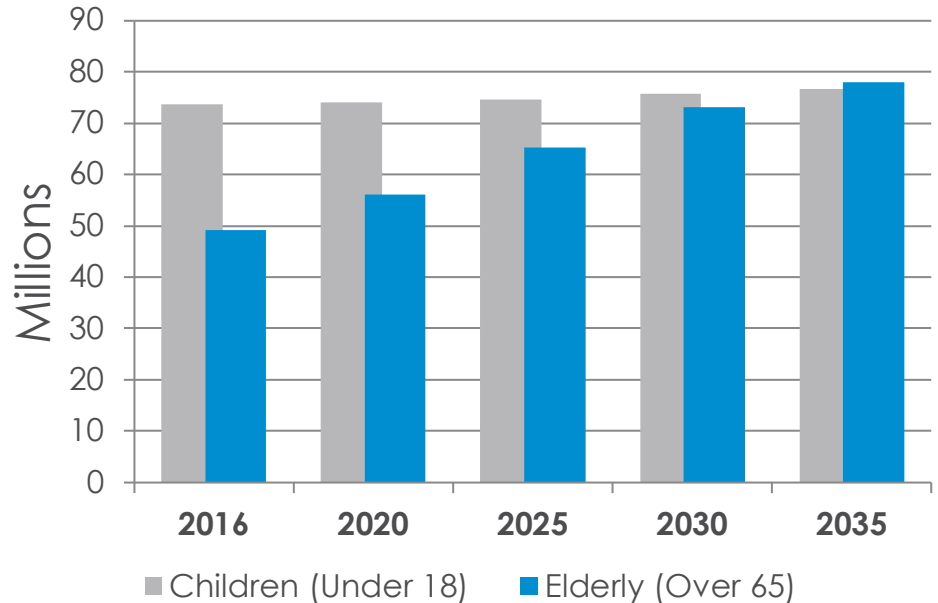
## By 2035

- According to the latest population projections, **adults 65 and older will outnumber children for the first time in U.S. history.**

## By 2040

- According to the latest population projections, the number of **adults 85 and older will increase by 126%.**

Elderly Population will increase **58%** by **2035**.



Source: U.S. Census Bureau

# State of Virginia

- There are currently **1.9 million Virginians** age 60 or older
- This will increase to **2.2 million** by 2030
- Virginia Adult Protective Services received over **39,000 reports of adult abuse**, neglect and exploitation during fiscal year 2021, which was a 5% increase from the previous year
- The good news is that Virginia has **ranked No. 4** for states with the best protections against elder abuse

# The Problem

- Approximately **\$28.3 billion** is lost each year to elder financial exploitation (AARP)
- In 2022, **3.1 million** people age 60+ were victims of identity theft, according to SeniorLiving.org
- Over **1 in 10** older Americans are victims of identity theft
- Seniors with **cognitive incapacity** suffer greater economic loss.

# Why are older adults targeted?

- **Age-related cognitive decline:** increased vulnerability due to diminished capacity to make sound financial decisions
- **Isolation and loneliness:** more susceptible to manipulation and exploitation
- **Dependence on others for care:** a reliance on caregivers or family members for financial management creates opportunities for abuse
- **Lack of digital literacy:** difficulty navigating online platforms and understanding potential risks





# How does financial abuse occur?

- ✓ In person
- ✓ Through the mail
- ✓ On the phone
- ✓ On the computer





# The Rise of Digital Abuse

- **Online Scams:** fake websites, investment fraud
- **Phishing Emails:** designed to trick elderly into revealing personal information or clicking on malicious links
- **Identity theft:** stealing personal information to access bank accounts and credit cards or opening new accounts
- **Telemarketing fraud:** deceptive sales tactics pressure older adults into unnecessary purchases or Medicare fraud
- **Social media scams/romance scams:** befriending older adults online and gaining their trust to exploit them financially

# On the Phone

## IRS / Government Agency scam calls

- The IRS or government agencies will NOT contact you by phone if you are late or have not paid taxes.  
[These are impostors!](#)

## Telemarketers

- Repetitive, high pressure calls sometimes including “scare tactics”
- Fake Charity Scams

## Medicare & Health Insurance Scams

- Scammers pose as Medicare representatives to get personal information
- Free or poor-quality medical supplies – billed to Medicare



# On the Phone

## The Grandparent/Family Member in Distress Scam

- A fake call from a grandchild, nephew, niece etc... saying they are in trouble and need money
- **NEW – Multistage scam** – “grandchild” asks grandparent to call defense attorney or local prosecutor with case number



# On the Phone - AI Voice Cloning

**ALERT! - Scammers only need 3-10 seconds of audio to clone a person's voice – audio clip from social media or voicemail**

## Most Common AI Voice Cloning Scams

- Fake kidnapping phone scams
- Grandparent scam calls
- Fake celebrity endorsement videos
- Scammers cloning your voice to access accounts
- Calls from friends who desperately need money

## Identifying an AI Voice Scams

- You only briefly “hear” your loved one's voice
- They can't answer simple questions
- You're called from an unknown number
- Someone else quickly takes over the call
- You're told to pay the ransom via cryptocurrency or gift cards

# Romance Scams & Artificial Intelligence

**Which of these social media profile pictures was generated by AI?**



# Romance Scams & Artificial Intelligence

- **Automated Messaging:** AI-powered chatbots engage with multiple targets simultaneously, initiating and maintaining conversations on dating platforms
- **Profile Creation and Personalization:** data analyzed to create fake personas tailored to appeal to specific demographics, featuring realistic photos, detailed biographies, and interests
- **Natural Language Processing (NLP):** used to generate convincing messages that mimic human speech patterns and emotions, establishing rapport and building trust with victims
- **Scam Detection Evasion:** to bypass detection systems implemented by dating platforms, continuously refining techniques to evade detection algorithms
- **Targeting Vulnerabilities:** high-potential targets identified by analyzing user data to identify individuals susceptible to romance scams based on online behavior, demographics, and psychological profiles

# Signs of Romance Scams

- **Love Bombing:** Showering the victim with excessive affection, compliments, and expressions of love to create a false sense of intimacy and attachment
- **Creating a Sense of Urgency:** Fabricating urgent situations or emergencies, such as a sudden illness or financial crisis, to evoke sympathy and prompt the victim to act quickly without questioning
- **Building Rapport and Trust:** Investing time in developing a rapport with the victim, sharing personal stories, and expressing empathy to create a bond and establish credibility
- **Mirroring and Validation:** Scammers mirror the victim's values, interests, and beliefs to create a false sense of compatibility and understanding. They validate the victim's feelings and opinions, making them feel validated and understood
- **Isolation Tactics:** Encouraging the victim to distance themselves from friends and family, thereby increasing dependence on the scammer for emotional support and guidance
- **Exploiting Loneliness:** Targeting individuals who are lonely or socially isolated, capitalizing on their desire for companionship and exploiting their emotional vulnerabilities for manipulation



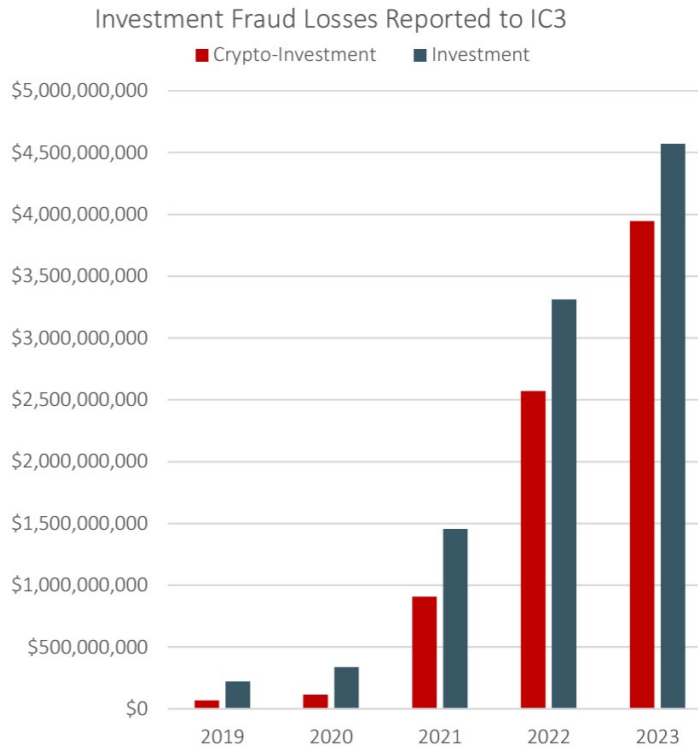
# Investment Scams

## Common Types of Investment Scams

- Affinity Fraud
- Ponzi Schemes
- Advance Fee Fraud
- Fake Charities and Nonprofits
- Cryptocurrency



# Investment Scams – FBI IC3 Report



## 2022 –

- \$3.31 billion in losses
- Cryptocurrency - \$2.57 billion

## 2023 –

- \$4.57 billions in losses
- Cryptocurrency - \$3.96 billion

# Investment Scams – Tactics Used

- High Pressure/Fear tactics
- FOMO – Fear of Missing Out
- Preying on cognitive decline
- Exploiting loneliness and isolation



# Investment Scams – Red Flags

Unsolicited  
investment offers

Pressure to invest  
quickly

Guarantees of high  
returns with little or  
no risk

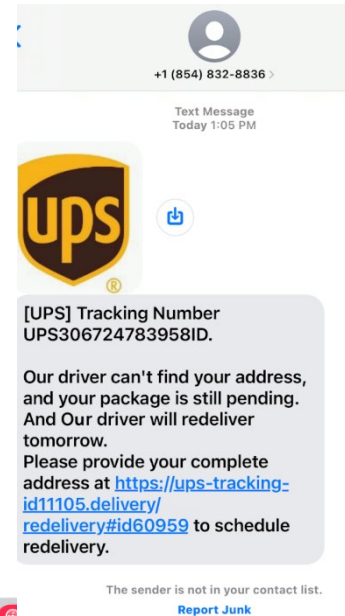
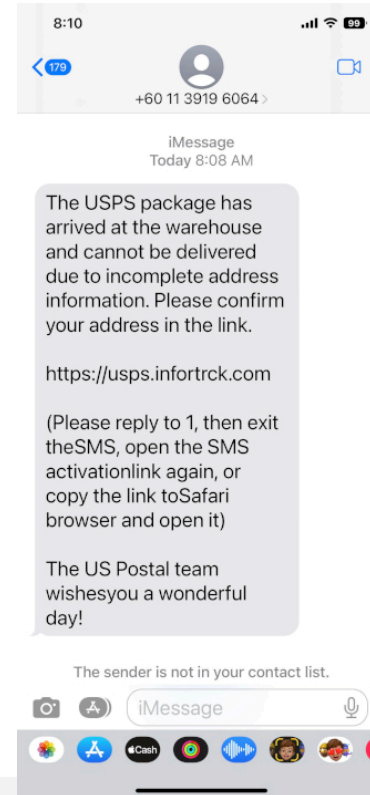
Requests for  
personal information  
or access to financial  
accounts

Lack of transparency

Too good to be true!

# Phishing/Smishing Scams

- Official-looking emails, ads or pop up messages designed to trick you into clicking on them
- Do not click these links — they may install a virus on your computer or take you to a false website to capture your personal data





**<http://safarianalyzer.windowsdesk.net>**

Safari - Alert

Suspicious Activity Might Have been Detected.

Major Security Issue

To fix it please call Support for Apple  
+1 888-476-6746 (Toll Free) immediately!

OK

# Anatomy of a Phishing Email

## 1. Asks for Sensitive Information

Dear Customer,

It has come to our attention that your account Billing Information records are out of date. That requires you to update your Billing Information. Failure to update your records will result in account termination.

Click on the reference link below and enter your login information on the following page to confirm your Billing Information records...

Click on [http://www.abc.com](#) to confirm your Billing Information records.

Thanks,



# Anatomy of a Phishing Email

## 2. Uses a Different Domain

The image compares a legitimate Amazon email with a phishing email. A red arrow points from the 'From' field of the phishing email to the 'From' field of the legitimate email, highlighting the difference in domains.

**Phishing Email (Left):**

----- Original Message -----  
Subject: Your Amazon.com order confirmation.  
Date: Tue, 7 May 2013 15:48:39 -0600  
From: Amazon.com <cheapskate@clients.amazon.ord>  
To: @lehigh.edu

Thanks for your order, @lehigh.edu!

Did you know you can view and edit your orders online, 24 hours a day? Visit [Your Account](#).

**Order Information:**

E-mail Address: @lehigh.edu

Billing Address:  
145-4938 In Road  
OH 43230-6107  
United States  
Phone: 1-242-246-4460

**Legitimate Amazon Email (Right):**

----- Original Message -----  
Subject: Your Amazon.com order confirmation.  
Date: Tue, 7 May 2013 15:48:39 -0600  
From: Amazon.com <cheapskate@clients.amazon.com>  
To: @lehigh.edu

Thanks for your order, @lehigh.edu!

Did you know you can view and edit your orders online, 24 hours a day? Visit [Your Account](#).

**Order Information:**

E-mail Address: @lehigh.edu

Billing Address:  
145-4938 In Road  
OH 43230-6107  
United States  
Phone: 1-242-246-4460

Amazon.com orders with the Amazon Visa Card. [Learn More](#)

1932039-7637560

> delivered to your Kindle or other device. You can view more information about this order by clicking on the title on [Amazon at Amazon.com](#)  
> a Robert B. Wyndle edition] \$ 60.99  
use Digital, Inc.

No Kindle Required. [Learn More](#) [Kindle](#) [Kindle](#) [amazonkindle](#)

irs in [Your Account](#). If you've explored the links on that page but still have a question, please visit our online [Help](#).

was sent from a notification-only address that cannot accept incoming e-mail. Please do not reply to this message.

ig with us.

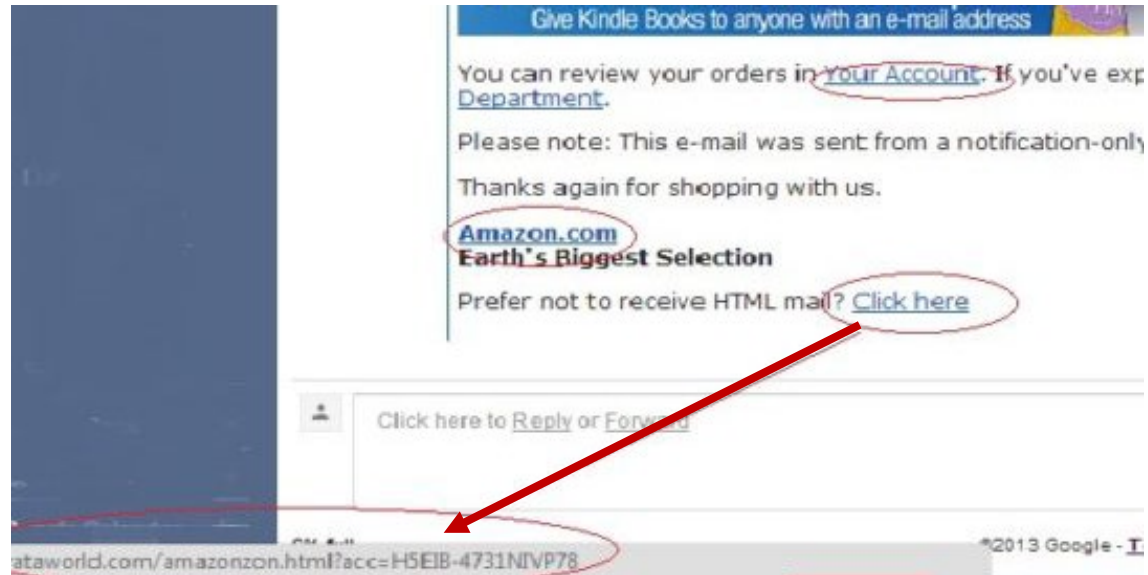
in  
L mail? [Click here](#)

Click here to Reply or Forward

©2013 Google [Terms of Service](#) [Privacy Policy](#) [Program Policies](#)  
Last account activity

# Anatomy of a Phishing Email

## 3. Contains links that don't match the domain



# Anatomy of a Phishing Email

## 4. Includes unsolicited attachments

Order Confirmation Inbox x

Arletha M. Paeth <willmarthcarey@gmail.com>  
to me ▾

Mon, May 27, 7:14 AM (1 day ago) ☆ 😊 ↶ ⋮


Thank you for your inquiry about account 96078306627951 for the period ending 27 May 2024. Our team is presently conducting research and will provide an update shortly VH8#AOGKMQ-0M-73SQR. If you require further assistance or have any questions, please reach out to us at WATARRLXDVFFHTI/CWD1CSYGVWYRJYNC8.


**Arletha M. Paeth**

Arletha M. Paeth

Isknynz-0f27e5c6-69c8-41e9-8f00-d625ac48f480


One attachment • Scanned by Gmail ⓘ

 Hello moelwar9@gmail.com,  
We appreciate your business. Your purchase has already been completed. Thank you for shopping with us. This transaction may take a few moments to appear in your account.  
Order Date: 27 May 2024  
Purchase ID: 0255121997454  
Invoice ID: INVOICE/2024/21544/GB1WL

 L2B3TERBEO5LC...

4:28 91 Order Confirmation

Arletha M. Paeth  
Isknynz-0f27e5c6-69c8-41e9-8f00-d625ac48f480

 Hello [REDACTED]@gmail.com,  
We appreciate your business. Your purchase has already been completed. Thank you for shopping with us. This transaction may take a few moments to appear in your account.  
Order Date: 27 May 2024  
Purchase ID: 0255121997454  
Invoice ID: INVOICE/2024/21544/GB1WL

**Order Details:**

Your order at bitcoin exchange.	\$463.47
(0255121997454)	
<b>Subtotal</b>	\$463.47
<b>Qty</b>	0.007 BTC
<b>Payment</b>	\$463.47

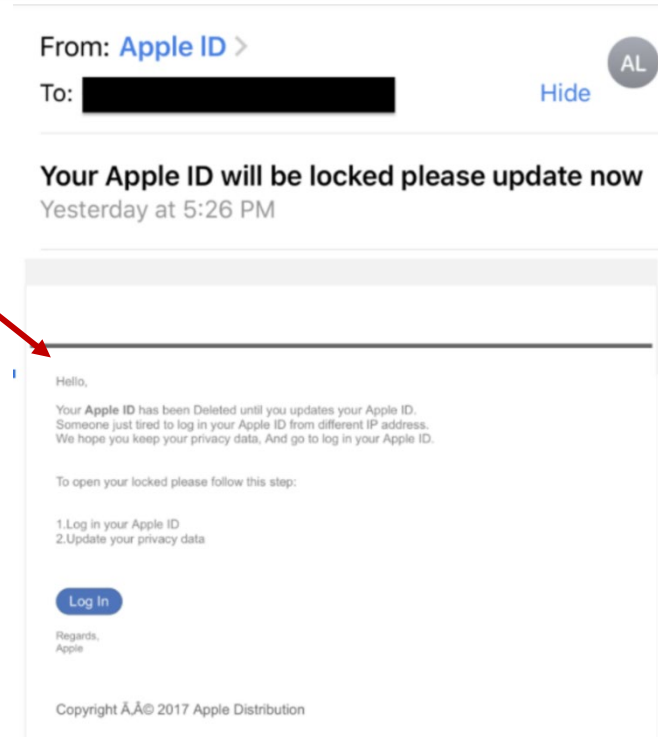
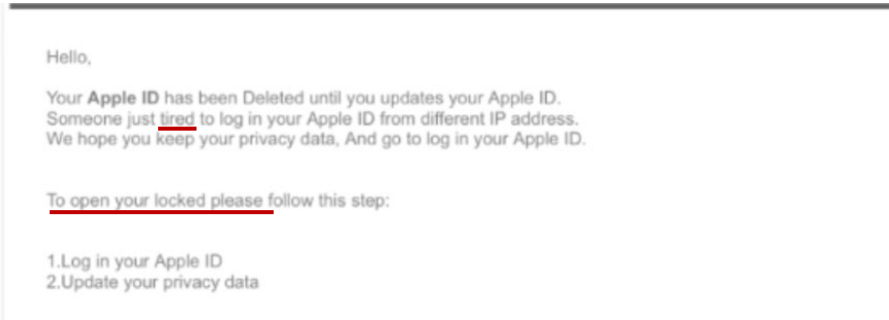
**Issue With this transaction?**  
You have 24 hours from the date of this transaction to open a dispute.  
**Customer Support Number: +1 (888) 224-0118**  
Please do not reply to this email. This mailbox is not monitored, and you will not receive a response.  
Copyright © 2024 PayPal, Inc. All rights reserved.  
PayPal, 5630 N. First St, San Jose, PayPal 94663, United States  
wvjkel-b4ab5242-d25c-467e-97f6-9c4a78aa55a



# Anatomy of a Phishing Email

5. Is not personalized

6. Uses poor spelling and grammar



# Anatomy of a Phishing Email

## 7. Tries to panic the recipient

Common phrases and tactics used:

- ✓ We've noticed some suspicious activity or log-in attempts
- ✓ There's a problem with your account or payment information
- ✓ You must confirm some personal information
- ✓ You need to make a payment
- ✓ You're eligible to register or receive a refund



Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: \$135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

<http://www.trustedbank.com/general/custverifyinfo.asp>

Once you have done this, our fraud department will work to resolve this discrepancy. We are happy you have chosen us to do business with.

Thank you,  
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.



# Tech Support Scams

- **Cold Calling:** unsolicited phone calls claiming to be from reputable tech companies, informing the victims of supposed issue with their computer or software
- **Pop-Up Messages:** deceptive pop-up messages that mimic legitimate system alerts, warning the victim of viruses, malware, or system errors and urging them to call a provided phone number for assistance
- **Remote Access:** a request for remote access to the victim's computer under the guise of troubleshooting or fixing issues, allowing them to install malware, steal personal information or manipulate the system



# Tech Support Scams



- **False Claims:** these are made about the presence of viruses, malware or security breaches on the victim's device to instill fear and urgency, prompting immediate action and compliance
- **Pressure Tactics:** using high-pressure tactics to coerce the victim into making payments or providing sensitive information, often claiming that failure to do so will result in severe consequences, such as data loss or legal action
- **Payment:** Often ask for payment by wiring money, gift card, pre-paid card, or cryptocurrency or money transfer app – all of which are hard to reverse



# Check Fraud

Financial Crimes Enforcement Network (FinCEN) reports that 2023 saw a significant increase in check fraud incidents and SARs (Suspicious Activity Reports) nearly doubled between 2021 to 2022 (350,372 and 683,541 respectively).

## Check Cooking

- Digital photos taken of stolen check; then using commercially available software to alter it

## Check Washing

- Criminals steal checks from post boxes and mailboxes and wash the checks with chemicals; leaving only the signature
- Guard against check washing by using gel-ink pens

## How to Stay Safe?

- Use credit cards for safer payments
- Mail check from inside the post office and continually monitor your account for suspicious transactions

# Red Flags of Digital Abuse

- Unexplained changes in spending habits or financial statements
  - Checks made out to “cash” or other people’s handwriting
  - Unexplained loans or sizable bank withdrawals
- New bills or debts OR unpaid bills or debt
- Second mortgages
- Mail no longer coming to the house
- Pressure to make hasty financial decisions or investments
- Reluctance OR anxiety/fear to discuss finances or share bank statements
- Unexplained changes in wills, power of attorney documents or beneficiaries
- Social isolation or changes in relationships with family and friends
- Unusual online activity or digital device usage



# Impact of Abuse

- Reluctance to end the abuse due to ties to the abuser (friend or family member OR new love interest), fear of retaliation, shame, dependency on the abuser for assistance, health care, or for economic reasons
- Physical & emotional suffering
- Losses – money, time, retirement income, homes/residence, self esteem, inability to provide for oneself

# Strategies for Prevention

- **Open Communication:** Encourage regular conversations with older adults about their online activities and concerns
- **Education and Awareness:** provide resources and training on common scams, online safety practices and password management
- **Empowerment and Support:** help older adults develop the confidence and skills to manage their finances online securely



# Strategies for Prevention

- Safeguard financial information
- Safeguard personal information
- Order FREE credit reports
  - Equifax, Experian, Transunion
  - Discuss FREE Credit Report Freeze
- Use Caller ID
- Never send/give money to someone you haven't met in person
- Encourage code words/phrases for family members
- Review all financial statements – monthly
- Set up of FREE fraud alerts – AARP Fraud “Watchdog Alerts” – email or text
- Ask for help - understanding financial transactions or if they are being pressured to give money or to sign a document

# Keeping Data Safe Online

- Create **Strong Passwords**
  - Consider a Password Manager App
- **Protect** Personal Information
- **Don't Click** on that link!
- **Two-Factor** Authentication
- **Secure** Social Media Accounts
- Maintain **Privacy**
- **Antivirus Protection**

 Cyber-Savvy Seniors

Content brought to you by:  
 Senior Housing Crime Prevention Foundation

### TIPS FOR KEEPING YOUR DATA SAFE ONLINE

Create Complex Passwords



Downloading a password manager will create and store encrypted passwords and protect your accounts by keeping your passwords in a secure location. Make a habit of also regularly changing your passwords.

Protect Personal Information



Never give out personal information over the phone or through text. Most agencies, organizations, and companies would never ask for such information in this manner.

Beware of Links



Be cautious before clicking on links! Hover over any hyperlinks you receive in email or on web pages to preview their locations. Hackers disguise hyperlinks to look legitimate so people are enticed to click on them.

Two-Factor Authentication



Always enable two-factor authentication on your accounts. It might be tedious, but this is an extra layer of security designed to ensure that you're the only person who can access your accounts, even if someone knows your passwords.

Update Regularly



Update your phone, app, and browser software as often as you can. These updates often include new security updates that your current software may not have.

more resources at: [shcpfoundation.org](https://shcpfoundation.org)



# SENIOR PLANET

FROM ~~AARP~~

## Classes -

Tech Discussion Group  
Protecting Personal  
Information Online

1-on-1 Personalized Tech Help

**[www.seniorplanet.org](http://www.seniorplanet.org)**

## Tech Tip Video Topics:

Setting up an Apple ID  
Downloading an App – Apple/Android  
Setting up a Gmail account  
Google Docs  
Hotspot – Apple/Adroid  
Instagram  
iOS 16 tutorials for Apple  
Privacy – Limiting tracking on Apple/Android  
...and many more



# Why is it Underreported?

- Shame and Embarrassment
- Fear of Retaliation
- Lack of Awareness
- Distrust of Authorities
- Complexity of Reporting Process
- Cultural and Social Stigma
- Lack of Support Services



# Reporting and Intervention

- Contact the **bank & credit companies**
- Put a **stop payment** on money wires or checks
- Place a **fraud alert** with the 3 credit reporting companies and **freeze the credit** reports
- Change your **phone number and passwords** to secure their finances
- **Shred** old credit cards and document with identifying information
- Call **law enforcement** and make a report

# Reporting and Intervention

- All fraud can always be reported to Adult Protective Services in your area:



**Virginia Department of Social Services:**

**Hotline: 1-888-832-3858**

**Website: [www.dss.virginia.gov/](http://www.dss.virginia.gov/)**

- Depending on the fraud type, you can report to the following services:
  - **Through the mail** – report to United States Postal Inspection Service (USPIS)
  - **Through the computer** – report to Sentinel, Federal Trade Commission (FTC), Internet Crime Complaint Center (FBI-IC3), or USPIS
  - **On the phone** – Contact the FTC
  - **On TV/Radio** – Contact the FTC
  - **In Person** – Call local law enforcement first



# Helpful Resources

## National Center for Victims of Crime (NVCV)

- <https://victimsofcrime.org>
- Victim Connect – 1-855-484-2846

## National Center on Elder Abuse

- <https://www.ncea.aoa.gov/index.html>

## US Postal Inspection Service

- <https://postalinspectors.uspis.gov>
- 1-800-275-8777

## National Association of Adult Protective Services

- [www.napsa-now.org/](http://www.napsa-now.org/)
- 1-217-523-4431

## AARP

- [www.aarp.org](http://www.aarp.org)
- 1-800-222-4444

## Better Business Bureau

- [www.bbb.org/scam-stopper](http://www.bbb.org/scam-stopper)

## US Securities & Exchange Commission

- [www.sec.gov/](http://www.sec.gov/)
- 1-800-732-0330

## Federal Bureau of Investigation

- <https://www.fbi.gov>
- 1-866-720-5721

## Consumer Financial Protection Bureau (CFPB)

- [www.consumerfinance.gov](http://www.consumerfinance.gov)
- 1-855-411-2372

# Helpful Resources

- **Credit Bureaus**
  - Equifax – [www.equifax.com](http://www.equifax.com) / 1-888-766-0008
  - TransUnion – [www.transunion.com](http://www.transunion.com) / 1-800-680-7289
  - Experian – [www.experian.com](http://www.experian.com) / 1-888-397-3742
- **FTC** - <https://www.ftccomplaintassistant.gov> / (202) 326-2222
- **Consumer Sentinel Network**
  - <https://www.ftc.gov/enforcement/consumer-sentinel-network>
- **FBI - Internet Crime Complaint Center (IC3)**
  - <https://www.ic3.gov/default.aspx>

# Helpful Resources

## CyberSavvy Seniors Handouts

- Gift Card Scams
- Tech Support Scams
- Data Safety Tips
- Phishing
- Smishing
- Power of Attorney
- Stopping Robocalls
- Top Scams Targeting Seniors Now
- And more!



# Credits

- Bureau of Justice Statistics
- National Institute of Justice
- US Census Bureau
- Consumer Sentinel
- AARP
- Financial Industry Regulatory Authority (FINRA)
- US Securities & Exchange Commission
- Federal Bureau of Investigation
- National Center for Victims of Crime
- National Center on Elder Abuse
- US Postal Inspection Service
- Federal Trade Commission
- National Adult Protective Services Association (NAPSA)
- Consumer Financial Protection Bureau (CFPB)

# Thank You



**Senior Housing Crime  
Prevention Foundation®**

8700 Trail Lake Drive Ste 140  
Memphis, TN 38125

[www.SHCPFoundation.org](http://www.SHCPFoundation.org)

Follow us on   



Marnie Stewart, President  
(877) 232-0859

[marnie.stewart@shcpfoundation.org](mailto:marnie.stewart@shcpfoundation.org)

