Fraud Prevention and Cybersecurity Seminar

Sponsored by: Leisure World Tech Center

President: Dave Merritt

Presented by:

Seth Hammerman, CISSP CCSP

Cybersecurity Professional

215-980-7999

Introduction – Why are Seniors the common target of scams?

- Scammers often target seniors due to their trust and financial security.
- Understanding scams is the first step to protecting yourself.

Some of the topics we will cover:

- **Telephone Scams** – How to recognize them and protect yourself
- **Email Safety** – How to spot and avoid a Phishing email
- **Smishing** – Avoiding scam texts
- **Social Media Safety** – Control the personal data you share on social media
- **"Check Washing"** and how to protect yourself

Questions for the Audience

- How do you use the Internet? Just Web browsing and email, or social media, online shopping/banking, etc?
- What are your main concerns about using the Internet?
- Have you ever had your identity stolen?
- Do you have antivirus software on your computer and update it on a regular basis?
- Do you know what a “Phishing” email is and how to spot one?
- What is Smishing? Do you know how to spot and avoid scam texts?

Anti Fraud and Information Security Tips For Seniors

Telephone Safety – Spot and Avoid Phone Scams!

Social Media Security – Don’t give away your Personal Information on Facebook, Instagram, etc. and make yourself a target for hackers!

Email Safety - Learn how to spot “Phishing” Emails and Avoid getting hacked or scammed!

WHAT IS IDENTITY THEFT?

Identity theft is the illegal use of someone else's personal information in order to obtain money or credit.

Tips

- Use a Password Manager instead of using the same password for every website
- Choose a password that means someone to you and you only; use strong passwords with eight characters or more that uses a combination of numbers, letters, and symbols.
- Do not reveal personally identifiable information online such as your full name, telephone number, address, social security number, insurance policy number, credit card information, or doctor’s name.
- Avoid opening attachments, clicking on links, or responding to email messages from unknown senders or companies that ask for your personal information.
- When making online donations, make sure any charity you donate to is a legitimate non-profit organization and that you type in the web address instead of following a link.
- Be sure to shred bank and credit card statements before throwing them in the trash; talk to your bank about using passwords and photo identification on credit cards and bank accounts.
- Check your bank and credit card statements monthly for unusual charges.

WHAT IS FRAUD? WHAT IS PHISHING?

Fraud *is the intentional perversion of truth in order to induce another to part with something of value or to surrender a legal right.* ***Phishing*** *is a scam by which an email user is duped into revealing personal or confidential information that the scammer can use illicitly or fraudulently.*

Tips

- Almost *all* organizations – banks, universities, companies, etc. - don't ask for your personal information over email. **Beware** of requests to update or confirm your personal information.
- Do **not** open attachments, click links, or respond to email messages from unknown senders or companies.
- **Don't** access your personal or banking accounts online from a public computer or kiosk.
- **Beware** of "free" prizes; if you think an offer is too good to be true, then it probably is.
- Make sure you change your **passwords** often and avoid using the same password for multiple accounts.
- Install and regularly **update** software firewall, antivirus, and anti-spyware programs. These software programs can help to protect the data on your computer, and can easily be purchased on the web or at your local office supply store.

Common Online Scams

- **Phishing Emails** – Fake emails pretending to be from banks, government agencies, or companies.
- **Tech Support Scams** – Calls or pop-ups claiming your computer has a virus.
- **Romance Scams** – Fraudsters pretend to be interested in a relationship to steal money.
- **Investment Scams** – Fake opportunities promising big returns. “Pig Butchering Scam” Leisure World Resident was a victim last year:Scam-costs-leisure-world-resident-800-thousand-dollars-man-arrested

Common Telephone Scams

- Medicare/Health Insurance Scams – Callers pretending to be from Medicare asking for personal info.
- IRS/Tax Scams – Threatening calls claiming you owe taxes.
- Lottery or Prize Scams – 'You've won! Just pay a fee to collect.'
- Grandparent Scam – Someone pretending to be a grandchild in distress.
- Tech Support Scam – "I'm calling from Microsoft, there is a problem with your computer!!"
- Unpaid Ticket Scam: "This is your local Police Department. There is a warrant for your arrest for unpaid tickets"

Telephone Safety

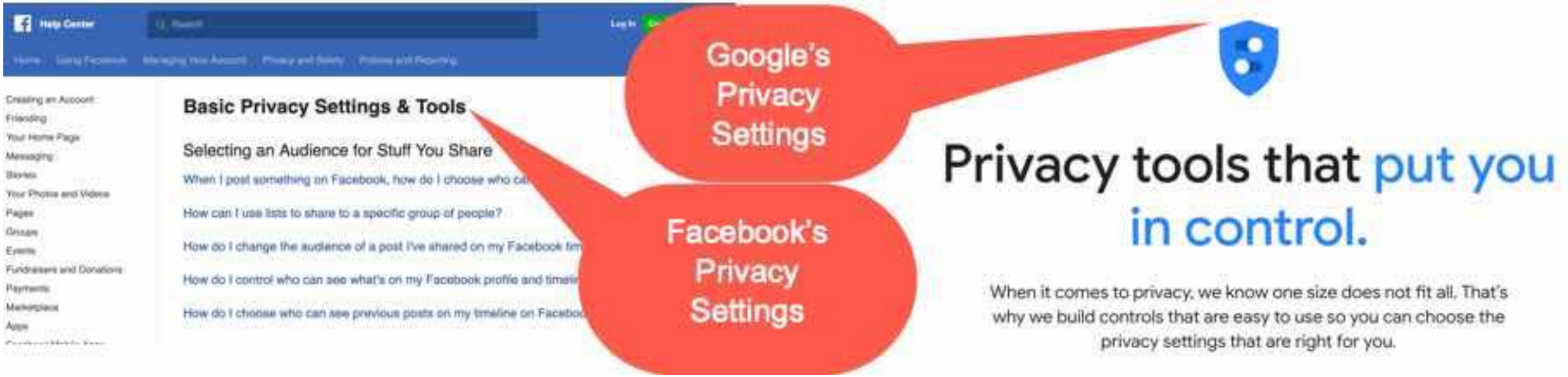
1st things 1st – The IRS, your Bank or Credit Union, Credit Card Companies, etc. are **NEVER** going to call you directly and threaten you, or ask for information!

Your Cellular Telephone Service Provider has Security software and/or services to help protect you from Robocalls, phone scam and more.

Remember – NO ONE will call you and demand information, money, or threaten you unless they are trying to scam you!

Social Media Safety

- 1st Rule of Social Media: Beware of what you share! ™ The bad guys are attacking Seniors on Social Media because they're the easiest targets!



Screen shot of Facebook & Google's Privacy settings pages. Make sure you check these settings on *all* social media sites!!

*Trademark of Hammerman Consulting, LLC

Phishing & “SMishing” Examples

Billing netflix 2020-08-10 21:48:25

S

Services <hicstnestle-gals14@yfgfzxxc.com>
8/10/2020 17:48

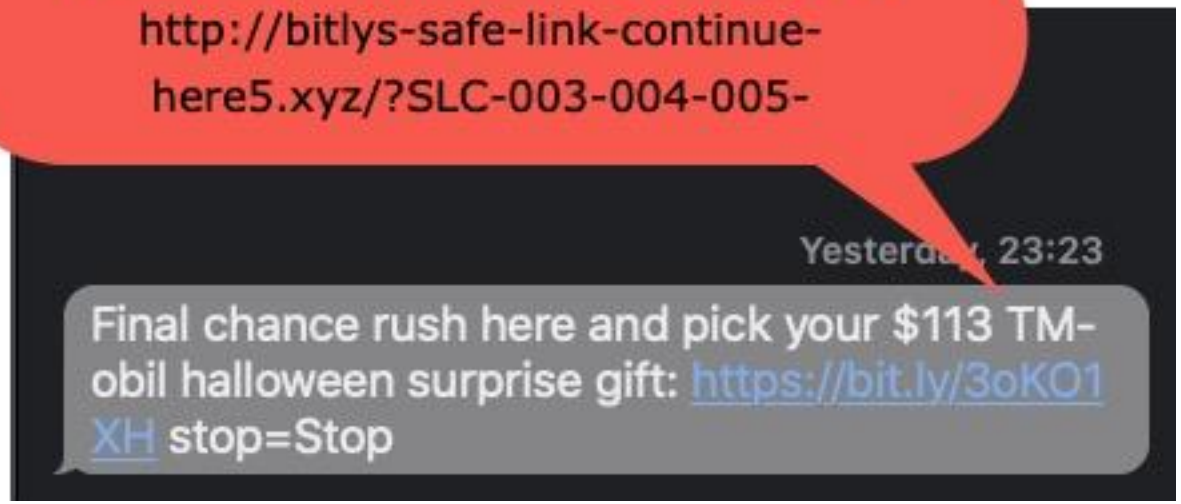
To: support@netflixteam.com

ALWAYS check the source address of the email!

NETFLIX

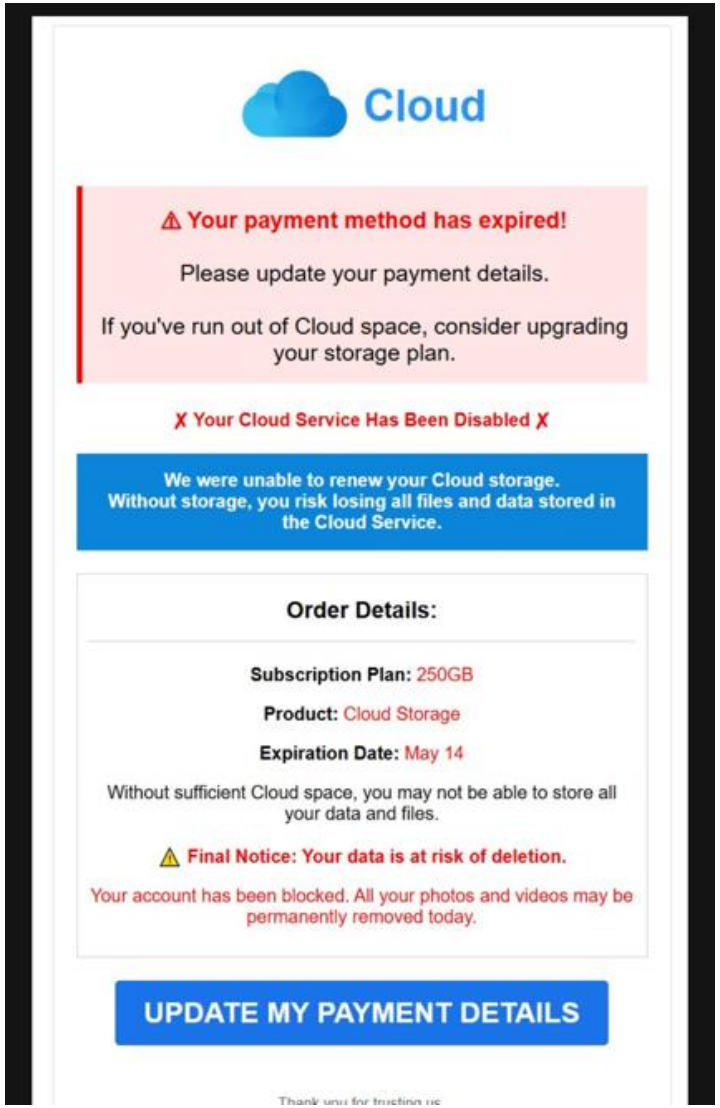
⚠ Your account is on hold.

T-Mobile is spelled “TM-obil and URL goes to http://bitlys-safe-link-continue-here5.xyz/?SLC-003-004-005-



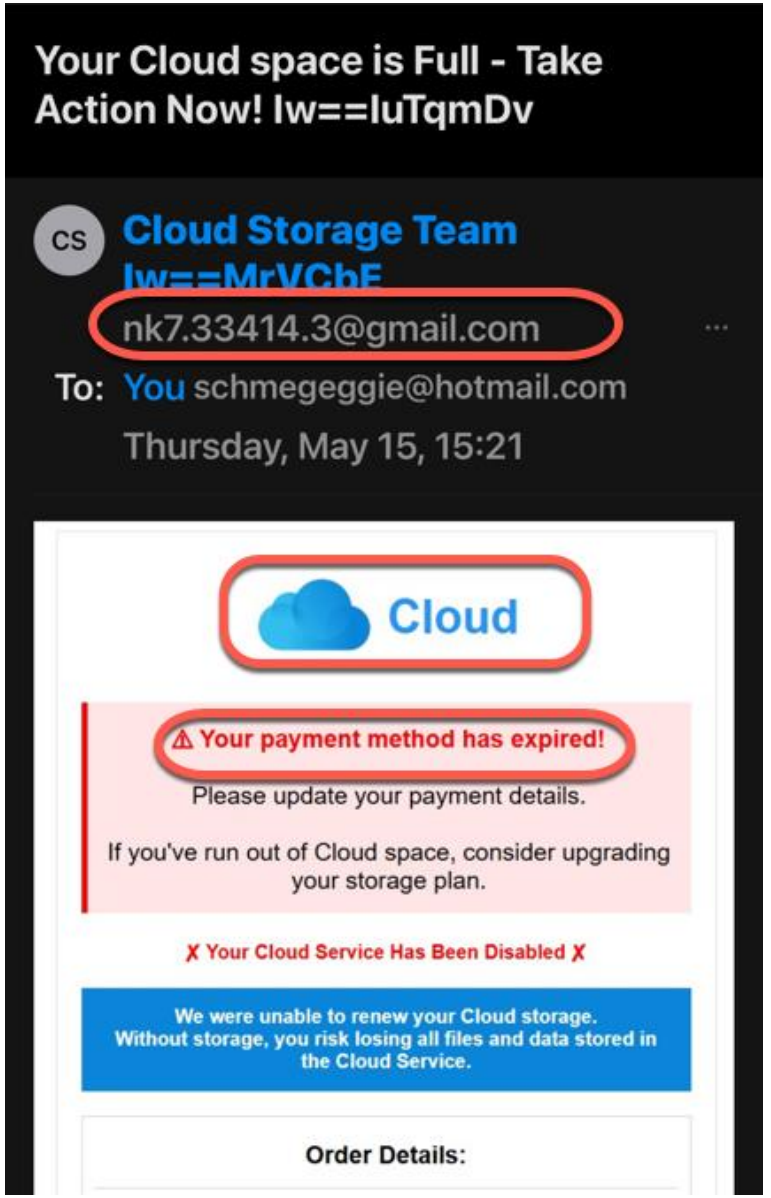
More Phishing Email Examples

- This is pretty good Phishing email, look at the graphic!
- But – there are still obvious ways to tell that it's fake.
- What do you notice that might be some telltale signs?

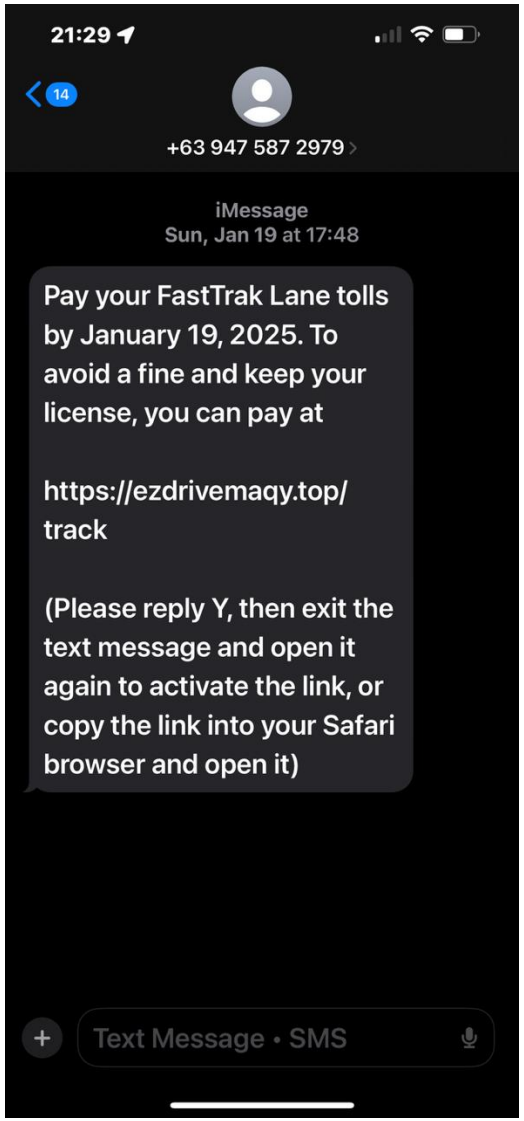


Phishing Email Example - continued

- Notice the nonsense characters?
- Take a close look at the return email address...
- Would an email EVER come from Apple, or Microsoft, from a Gmail address?
- Notice the sense of urgency. EVERY Phishing email is trying to create it.
- ALWAYS be suspicious of these kinds of phishing emails, no matter how serious they sound!!



More Examples of Smishing Messages



These are **actual smishing texts** I've received on my phone

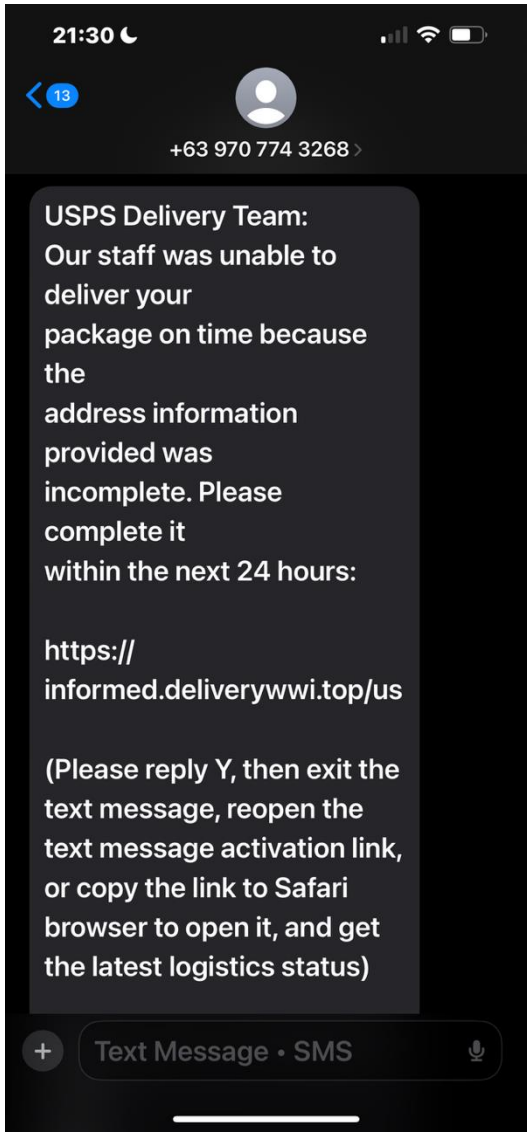
What are some telltale **signs** that tell you that these are fakes?

Always look at the phone number or email of where the text comes from

Look at the URL where it's trying to get you to follow

Also understand the domain of that website – is it really the E-Z Pass or Fast Trak Authority?

Is that really the web page of the US Postal Service?



Check Washing

Check washing is a form of financial fraud where a scammer steals a check, removes the ink using chemicals, and then alters the details such as the payee name and amount before cashing it. This can result in significant financial loss for the victim.

How It Works:

1. **Stealing the Check**: Scammers often steal checks from mailboxes or collection boxes.
2. **Washing the Check**: They use chemicals like acetone or bleach to remove the ink, leaving only the signature.
3. **Altering the Check**: The scammer then fills in their own name and the desired amount

Prevention Tips:

- Use **black gel pens** with indelible ink, which is harder to wash off.
- Mail checks directly at the **post office** instead of using standalone mailboxes.
- **Collect your mail promptly** and consider holding it at the post office if you're away.

How to Recognize Scams

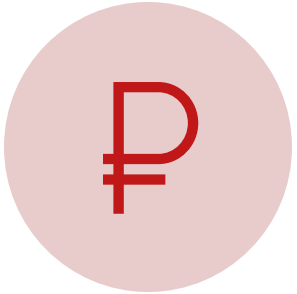
- **Sense of urgency** – Scammers often try to rush you into making decisions. This principle is a key aspect of “social engineering.”
- **Personal information requests** – Legitimate banks and government bodies will never contact you to ask for your Social Security Number or passwords.
- **Offers that seem too good to be true** – If an offer appears overly attractive, it is likely a scam.
- **Uncommon payment methods** – Requests for payment via gift cards, wire transfers, or cryptocurrency should raise suspicion.

Protecting Yourself Online

• **Never** click on ANY links in emails.

• Use a password manager, strong passwords and enable two-factor authentication.

• Keep software and antivirus protection updated.



• Verify charities and investment opportunities before donating.

USING THE INTERNET SAFELY

Email, instant messaging, and personal websites now provide easy ways for everyone to stay connected, informed, and involved with family and friends. The Internet also provides an easy way to shop, plan travel, and manage finances.

Many scammers target Americans ages 65 and older via emails and websites for charitable donations, online dating services, online auctions, buyer's clubs, health insurance, prescription medications, and health care.

Many of the crimes that occur in real life – happen on the Internet too. Credit card fraud and identity theft, embezzlement, and more – all can be and are being done online.

At home, at work, and in the community, our growing use of technology, coupled with increasing cyber threats and risks to our privacy, demands greater security in our online world.

RESOURCES AVAILABLE TO YOU

- ***AARP:*** The AARP provides specifics on internet safety, how to protect your privacy, and the most up-to-date virus protections.
- ***FBI:*** This is a list of common fraud schemes aimed at older Americans.
- ***SeniorNet.org:*** SeniorNet offers computer training at senior centers, public libraries, schools, and hospitals as part of their mission to provide older adults computer technology education.
- ***Fraud.org*:** Fraud.org helps protect consumers from being victimized by fraud.
- ***FTC's PassItOn Campaign***: The PassItOn Campaign enlists people 65 and older in an effort to recognize and report fraud and other scams. Topics include imposter scams, identity theft, charity fraud, health care scams, paying too much, and "you've won" scams.

Some Cybersecurity Product Resources

- **Password Managers:**
    - NordPass
    - 1Password
    - Dashlane
- **AntiVirus/Malware Protection Platforms**
    - Avast One
    - Bitdefender
    - Malwarebytes Premium
- **VPN (Virtual Private Network) Clients** – A VPN “hides” your information while browsing sites on the Internet so that your private information is protected
    - NordVPN
    - SurfShark
    - ProtonVPN

Note – These are just a few examples of vendors, NOT recommendations. You need to choose products yourself that are a fit for you based on your experience

Thank You!

Learn more online at:
https://states.aarp.org/maryland/tag/fraud-watch-network