

The background features a light gray circuit board pattern with black lines and circular nodes. A dark gray horizontal band runs across the middle of the image, serving as a backdrop for the text.

Cyber-Safety Considerations for Seniors

Protect Your Online Presence

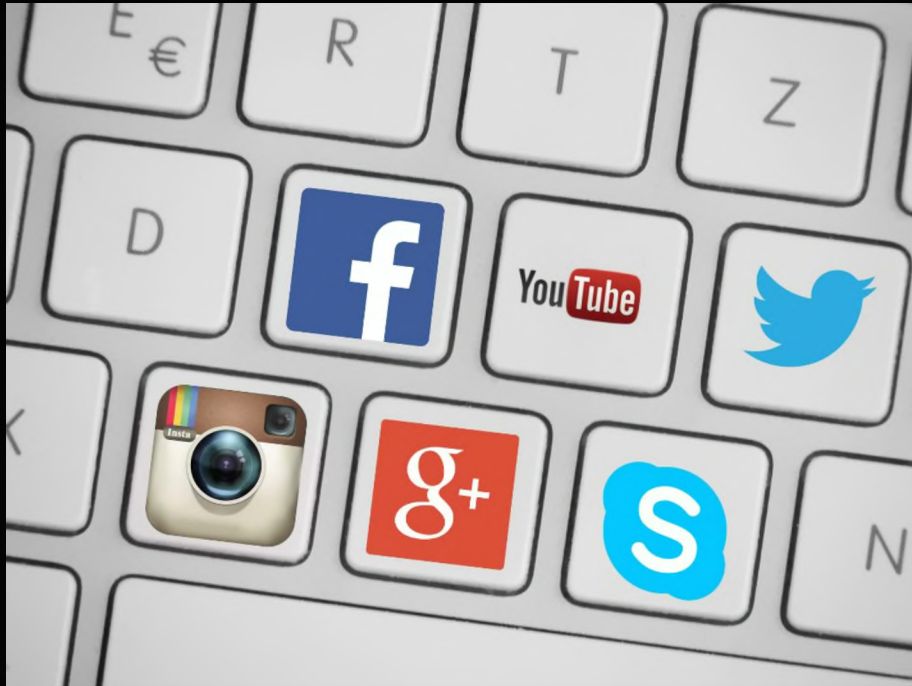
Agenda Item VII C (SILVER)
Meeting Date: 11-13-19

Why are Seniors Targets for Scams?

- Immediate funds available (retirement/savings account)
- More likely to live alone
- Not as likely to report scams



Social Media Dangers



- Location data
- Your Family Members
- Your Routine
- Your Lifestyle/Assets
- Password/security question information
- Personal Information generally

Social Media Tips and Precautions

- Spend time exploring privacy controls
- Consider limiting your friends list.
- Think carefully about what you share
- Change your tagging controls
- Messenger – Not confidential; be careful about clicking on links.



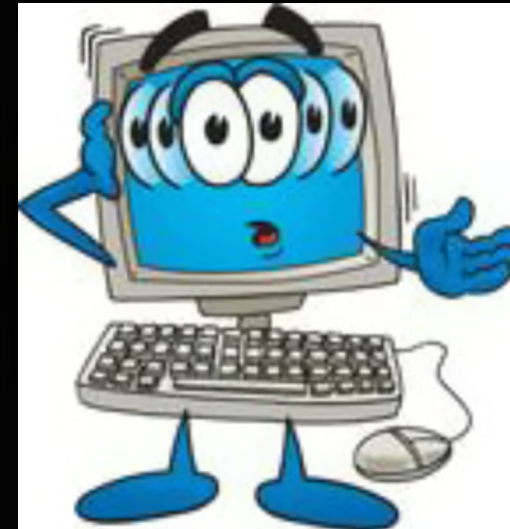
Internet of Things



- The interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data
- Thermostats, televisions, alarm systems
- Smart speakers: Amazon Echo (Alexa) and Google Home
 - Turn off your Echo's mic; mute Home or turn off
 - View and delete your dialogue history (Echo and Home)
 - Check your “drop-in” settings (intercom system with other Echoes)

Common Methods of Cyber ID Theft

- Phone, Mail, or e-mail Scams
- Malware
- Data breaches of Companies with Your Personal Information
- Skimmers
- Good Ol' Fashioned Theft



How Criminals Use Your Information

- Open New Accounts in Your Name
- Create Counterfeit Payment Cards Linked to Your Account
- Create pre-paid cards with your information
- File False Income Tax Returns
- Fraud May Occur Immediately, or in the Future.



Trends in phone, mail, and email scams

- Utilities/IRS phone scam – A person calls you saying your utility will be shut off or that you owe taxes and you will be arrested unless you wire money. There are many variations of this (friend in jail/hospital/stuck overseas/immigration).
- Phishing – E-mail message that appears to be from a trustworthy source, but is actually someone trying to obtain your personal information
- Tech Support Scam – Someone calls claiming your computer has a problem. Scammers asks to connect to fix it.

Grandparents Scam



- Always be cautious of anyone who calls you demanding money.
- Use a family code word.
- Call family member directly, or someone close to them.
- Be cautious if someone asks you to pay by wire transfer or reloadable debit card. Treat it like cash – once it's gone, it's gone.

Skimming Devices



Skimmers and identity theft

- A skimmer is a device used to copy payment card numbers and personal identification numbers (PINs). Skimmers are installed at merchant locations, point-of-sale (POS) devices, automated teller machines (ATM), and stand-alone kiosks.
- Most skimmers are very difficult to spot, even for law enforcement

Tips for spotting ATM and Gas Skimmers

- ATM skimmers are attached on or around ATMs.
- Gas pump skimmers can be installed externally over the card reader or internally.
- Inspect the terminal for any signs of tampering.
- Look for the following: a card slot that is loose or has fallen off; the presence of double-sided tape, glue, or pry marks around the card slot.

Skimmers: Minimizing your risk

- Cover the PIN pad while you enter your PIN.
- Use a credit card.
- Be especially vigilant when withdrawing cash on the weekends.
- Monitor your bank statements.
- Pay for gas or pull out cash inside

What to do if you are a victim of a scam

- Notify creditors
- Place a fraud alert with credit reporting agencies (now 1 year)
- File a report with your local police
- File a complaint with the Federal Trade Commission

<https://www.ftccomplaintassistant.gov>

- Credit freezes are now free



Credit Reporting Agencies

- Equifax

- [Equifax.com/personal/credit-report-services](https://www.equifax.com/personal/credit-report-services)

- 1-800-685-1111

- Experian

- [Experian.com/help](https://www.experian.com/help)

- 1-888-397-3742

- TransUnion

- [Transunion.com/credit-help](https://www.transunion.com/credit-help)

- 1-888-909-8872

Organizations to Contact

- Federal Trade Commission (FTC)
 - [FTC.gov](https://www.ftc.gov) and (202) 362-2222
- Treasury Inspector General (IRS Scams)
 - www.treasury.gov and (800) 366-4484
- Nevada Attorney General
 - nv.ag.gov and (775) 684-1100