Online Self Defense
White Belt Level
Assessing Your Risk

Impact

Ease of Exploitation
Malware

Back Doors  Ransomware
Scareware
Spyware
Bloatware
Adware
Phishing and Spear Phishing
Avoiding Phishing

- Identify phishing emails
- Never click on links in emails
- Be suspicious of email attachments
- When in doubt contact the company that an email claims to be from
Phishing Response

• Do Not click on any links
• Forward the email to spam@uce.gov
• Contact the bank or company that the email claims to be from to alert them
• Do Not respond to the email
Update ALL of your software

98% of software exploits are already fixed
Windows Updates

Start button → Control Panel → Systems and Security → Windows Updates
Which Antivirus software to use

- Cost
- Ease of Use
- System Resources
Backups

3-2-1 Rule

3 Copies of data

2 different types of media

1 copy offsite
Passwords

A Long password is a strong password

- **Password 1 “%Ab3$9”**
  - 6 Characters, uses upper case (26), lower case (26), numbers (10) and special characters (36)
  - Possibility of guessing is 1 in $98^6$ or $885,842,380,864$

- **Password 2 “Correct Horse Battery Staple”**
  - 28 Characters. Uses upper case (26), lower case (26) and Spaces (1)
  - Possibility of guessing is 1 in $53^{28}$ or 1 in $190,425,168,600,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000$
Safely Storing Passwords

- Write it down
- Use a password vault
- Use two factor authentication
Questions

Chuck McAndrew
Chuck.mcandrew@leblibrary.com