Basic Computer Security Checklist

As you complete each task check the corresponding box

- ❑ Install and enable the (Software) auto-update features in your OS (Mac – Windows)
- ❑ Use the OS Firewall (It should be on by default (But make sure to check) (Mac – Windows)
- ❑ Install, update and run (At least weekly) anti-virus software (free tools are available)
- ❑ Install, and update all third-party software (Adobe, Java, etc.) (Mac – Windows)
- ❑ Install, update and run MalwareBytes (Malware removal tool - Windows and Mac)
- ❑ Always use a Virtual Private Network (VPN) when connecting to an untrusted network. (Open or free Wi-Fi)*
    - (PIA is good: https://www.privateinternetaccess.com/pages/buy-vpn/)
- ❑ Use a strong password (Passphrase is better, multi-factor is best) at least 8 characters, upper and lower case, 1 special character and a number. Do not reuse the same password on multiple sites. (Use a password manager to manage your passwords.)
- ❑ Do not open any attachments or click on any links in an email unless you are expecting them. (Ask before you click)
- ❑ No reputable institution (Education, Financial, Government, etc.) will ever ask you for your personal information in an email. (Password, username, SS#, credit card number, etc.).
- ❑ Do not install random software from the Internet. ("Free software" = Malware).
- ❑ Before installing software on your mobile device consider whether it's reasonable for the application to have access to your personal information. (Photos, GPS, storage, contacts, etc.)
- ❑ Use a password (or biometric) for your mobile device to secure it from unauthorized access.
- ❑ Don't run as Administrator – Run as a normal user with non-administrative privileges. It is much easier for Malware to do harm when you run as an Administrator.
- ❑ Use a separate "clean machine" for your financial business (Bill pay, purchasing items online, etc.). Use another device for casual browsing and other online entertainment.
- ❑ Shutdown your computer if you are not using it for more than a day. (Saves energy and reduces your attack surface) (If they can't find you, they can't "Pwn" you…)
- ❑ Set up a separate email account for dating sites, mailing lists, coupons, etc. Never use you work email for personal use.
- ❑ Always create a backup of your important information. (Think Ransomware… ☹)
- ❑ Encrypt your devices – computers, laptops, tablets, and mobile devices, etc. (Would you hand your unlocked cell phone to a stranger and walk away?)

Protecting Your Identity

- ❑ Get an IRS PIN: https://www.irs.gov/individuals/get-an-identity-protection-pin
- ❑ Register with Social Security: https://www.ssa.gov/myaccount/
- ❑ Protect your identity AARO, LifeLock, etc.: https://www.aarpidprotection.com/
- ❑ Have I been Pwned: http://haveibeenpwned.com
- ❑ OpenDNS: http://www.opendns.com
- ❑ Find My iPhone (Use safari) http://www.apple.com/icloud/find-my-iphone.html
- ❑ Find my phone Google https://www.google.com Type: /Find my phone
- ❑ Prey https://preyproject.com/
- ❑ LastPass Personal: https://lastpass.com/

Free Software (For Home Use)

Antivirus Tools

1. **Sophos (Antivirus Software, Mac, PC)** https://home.sophos.com/reg

2. **Avira (Antivirus Software, Mac, PC, Android)** http://www.avira.com/en/free-antivirus-windows?x-c-channel=CJ&x-a-source=affiliate&x-a-medium=7260568

3. **AVG (Antivirus software, Mac, PC, Android)** http://www.avg.com/us-en/avg-antivirus-for-mac?dsc=ah1&d=50&h2=50&subh2=50&ECID=ad:go:se:US-EN-XSite-Brand-Search&gclid=Cj0KEQjw4fy_BRCX7b6rq_WZgI0BEiQAl78nd6nwy2Fv0tyb3tXjBUA_A7eLDtacSj8_TVYS2Lo21pMaArlo8P8HAQ

4. **Avast (Antivirus Software, Mac, PC, Android)** https://www.avast.com/

5. **Panda (Antivirus Software, Windows only)** http://www.pandasecurity.com/usa/homeusers/solutions/free-antivirus/

6. **Bitdefender (Antivirus Software, Windows only)** http://www.bitdefender.com/solutions/free.html

7. **Windows Defender (Built-in Antivirus) (Very good AV, Includes ATP)** https://www.microsoft.com/security/scanner/en-us/default.aspx

Malware Tools

1) **MalwareBytes (Windows and Macintosh)** https://www.malwarebytes.com/mwb-download/thankyou/

2) **Malicious Software Removal Tool (Windows only)** https://www.microsoft.com/en-us/safety/pc-security/malware-removal.aspx

3) **Spybot (Windows Only)** https://www.safer-networking.org/mirrors24/

4) **Kaspersky (Windows Only)** http://usa.kaspersky.com/free-virus-scan

Ransomware

"Ransomware Rescue Kit"

a. https://bitbucket.org/jadacyrus/ransomwareremovalkit/overview

b. https://www.decryptcryptolocker.com/

c. https://noransom.kaspersky.com/

Browser based VPN and Proxy

1. **Opera (Web Browser with built-in Ad block and VPN)** http://www.opera.com/?gclid=CJqe9b75188CFQltfgoddfoNVQ
   - **Make sure to check perform the Webrtc leak test.** http://www.ghacks.net/2016/04/23/block-opera-vpn-from-leaking-your-ip-address/
2. **EPIC (Web Browser with Proxy, VPN and ad-blocker built-in)** https://www.epicbrowser.com/

For Your Children

- Protect your children's identity:
  - https://www.fbi.gov/news/stories/fbi-releases-new-version-of-child-id-app (provides parents with an easy way to electronically store their children's pictures and vital information to have on hand in case their kids go missing.)
  - https://www.consumer.ftc.gov/articles/0040-child-identity-theft
  - https://www.consumer.ftc.gov/topics/protecting-kids-online
  - http://www.parenting.com/article/keeping-your-child-safe-on-the-internet
  - https://www.fbi.gov/resources/parents/resources-for-parents

*Web Portal does not mean security. A Web Portal can simply be an electronic toll booth allowing access but no security.