CYBERSECURITY: Home/Personal Devices and Teleworking

In response to COVID-19, the State has taken the unprecedented approach of encouraging all employees who can, to telework to create social distancing. This document is intended to help you succeed at that task in **FIVE** easy steps. All links in this document are clickable.

Prepare your personal device and network with security in mind.

#1 Patch your desktop and/or laptop for both the Operating System and Applications.

- Windows 10: Windows Support: Update Windows 10
- MacOS: Apple: How to update the software on your Mac
- If you don't have Windows 10 or a Mac, please Google how to update your specific operating system and follow those directions.

#2 Use **STRONG** passwords for all your personal logins. Where possible, use Multi-Factor Authentication.

Don't let the name fool you, "HaveIBeenPwned" is a very useful website for checking to see if your personal email addresses have been exposed in a data breach(s) and testing the your passwords to see if they are strong and part of an existing previously exposed or known password dictionaries.

#3 Use a modern browser that is up to date. All of the browsers listed below will work well with Office 365:

- Chrome – How to Update Google Chrome Help: Update Google Chrome
- Firefox – How to Update Mozilla Support: Update Firefox to the latest version
- Microsoft Edge – Updated through Windows 10 Updates
- Safari – Updates included with MacOS updates

#4 Have an update-to-date and modern Antivirus software installed. There are options that are free and very effective. None of this is supported by the System Office.

- On Windows 10, make sure Windows Defender is enabled and updated. This can coexist with other AV software.
- If you're a Spectrum customer, you can get a free Security Suite (current subscription required): Spectrum: Download and install security suite for Windows
- Other capable free AV solutions:
- Windows: AV Test: The best Windows antivirus software for home users
- Mac: (yes, you're not impervious to viruses and malware!) AV Test: The best MacOS antivirus software for home users
- Avira, Avast, AVG and Kaspersky and all are good to excellent free and paid options.
- There are excellent paid solutions available also like Norton, McAfee and others.

#5 Consider enabling/configuring a DNS security filter on either your personal device or your entire home network. This requires some hands-on changes on desktop/laptop or router but should be easy enough for most people to accomplish. Doing this will offer additional protection against malware and ransomware beyond just working at home.

Updated March 16, 2020

CYBERSECURITY: Home/Personal Devices and Teleworking

DNS Security Filter continued…

Quad 9 (9.9.9.9) is a FREE, set it and forget it, DNS security filter. At Quad9 there are instructions (video and text) on how to configure your DNS for both Apple and Microsoft operating systems.

OpenDNS is another security and privacy DNS tool with a free service for home and paid services for additional tiers. OpenDNS allows for greater control with customizable filtering and basic protection.