Personal Computer Security Checklist

Computer/Laptop Security

❑ Is your operating system up-to-date	Windows and Apple operating systems will have settings that allow the automatic download of patches and updates. Allowing automatic installation of the updates is up to you, but at least enable to auto-download and notify.
❑ Do you have an antivirus installed	For Windows-based systems, Windows Defender is adequate. Avast is a highly-rated program with versions for multiple operating systems (Mac, Windows & Android). Kaspersky is also highly-rated but has been banned from Federal networks due to security concerns. As with your OS, make sure your antivirus remains up-to-date.
❑ Are the applications you use up-to-date	Not all programs have an auto-update option when a newer version is available and you may need to check on your own. If a developer no longer supports a program you use, consider finding a replacement.
❑ Have you rebooted your computer recently	While some updates don't require a restart to take effect, a majority will. For updates that require a restart, you will generally get a notification to this effect. If you leave your computer on when not in use, get in the habit of restarting on a regular basis to make sure everything is truly updated.

❑ Is your information securely backed-up	A new trend in malware is ransomware. These attacks will encrypt all the data on your hard drive and will demand payment to provide the decryption key. Without this key, your data is lost forever. If you have your data backed-up, you can wipe the hard drive and reinstall. There are online back-up services and you can also buy desktop hard drives to do the same – make sure the back-up is not connected to your computer or it will be encrypted as well.

Web Browser Security

❑ Do you have an ad-blocker installed	Malicious advertisements are increasingly being used to infect computers. There are multiple, reputable, options for ad-blockers depending on the browser you are using. Adblock Plus is available for Internet Explorer, iOS, and Firefox. uBlock Origin is available for Chrome, Firefox, Safari, Opera, and Edge (Windows 10 browser).
❑ Is your web browser up-to-date	Yes, this is a theme. Browsers are updated to fix exploits and improve operation often. Enable automatic downloads of updates and restart your browser after installation.
❑ Use private windows	Most browsers will come with a privacy-browsing option: InPrivate browsing for IE, Incognito for Chrome, etc. Familiarize yourself with these options and use them when accessing sensitive information. Private windows prevent malicious code in other tabs from "seeing" or interfering with what you are doing in a private window.

❑ Use https:// when available	Https is a secure, encrypted connection from your computer to a website. Many services offer encrypted and unencrypted versions of their website and most will default to secure https when you are on the login screen. You can confirm if you are viewing the encrypted website by the presence of a green lock icon or seeing **https** in the web address. While https will not protect your information on an already-compromised computer, it will prevent someone from snooping on the connection between your computer and a website. If you do not see the green lock, you can manually enter https:// as part of typing a URL to force the secure connection if it is available. There is also an extension called HTTPS Everywhere that is available for Chrome, Firefox, Opera, and Edge that forces the use of the encrypted option on supported websites.
❑ Disable Flash	Flash is a popular vector to attack computers. If you cannot disable Flash, at least set it to "Ask first" – this will prevent flash from running automatically when a webpage loads. In most browsers this is a default setting, but check to make sure it is enabled.

Password Security

❑ Don't reuse passwords	The use of the same password across multiple services means if any of those services are compromised, hackers can get into those other accounts as well. Make sure every password is unique to the service/site you are using it for.
❑ Don't answer security questions	Security questions are often publicly available information – mother's maiden name, elementary school, etc. If the information is out there, someone can use it to "recover" your password without needing to place malware on your computer. If a site insists on providing such answers, don't answer truthfully.

❑ Use multi-factor authentication when available	Many services are moving towards providing some sort of multi-factor authentication – Facebook and Gmail are such examples. The second authentication factor will prevent someone from accessing your information even if they have your username and password. In some cases, sites will notify you of the attempted login which will alert you to the potential compromise.
❑ Use long passwords	Increasing password length from 8 characters to 9 increases the amount of time needed by an automated password cracker from minutes to hours. Adding a 10^{th} character will up that time to days. It is highly recommended that you make sure passwords are 12 characters or more. Even if a website or service doesn't require special password security (symbols or numbers), get in the habit of doing so anyway.
❑ Consider using a password manager	We choose poor passwords because we need to think of them and make them easy to remember. A password manager removes both of these concerns. There are secure online options like LastPass or 1Password that encrypt your passwords locally before saving them to the cloud. There are local password managers like Keepass that will save everything to your machine so you do not have to worry about cloud security, but you will need it separately on each device you use. You will still need a strong master password for access, it's easier to come up with and remember one strong password than fifteen.