WESLEYAN UNIVERSITY ***Basic Computer Security Checklist*** **TRINITY COLLEGE**

- ❑ Install and enable the (Software) auto-update features in your OS (Macintosh – Windows)
- ❑ Use the OS Firewall (It should be on by default (But make sure to check))
- ❑ Install, update and run (At least weekly) anti-virus software (free tools are available).
- ❑ Install, and update all third party software (Adobe, Java, etc.)
- ❑ Install, update and run MalwareBytes (Malware removal tool - Windows only).
- ❑ Always use a VPN when using an untrusted network. (Open or free WiFi)
- ❑ 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 LastPass 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 (Edu, 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 that application ***to have access to your personal information***. (Photos, GPS, storage, 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 steal your data)
- ❑ 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.
- ❑ Encrypt your devices – computers, laptops, tablets, and mobile devices, etc.
- ❑ 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 children's identity: https://www.consumer.ftc.gov/articles/0040-child-identity-theft
- ❑ Protect your identity AARO, Lifelock, etc: https://www.aarpidprotection.com/