System Hardening

1. Device guard: Device guard will lock your device down so only trusted applications that the user defines in code integrity policies.

2. BitLocker: BitLocker makes it so your files on a selected drive become encrypted, I encrypted all my important files on my secondary drive. 

3. Disabling remote access: Disabling remote access to your computer makes it more difficult for people to access your files and commuter through remote access. 

4. Disabling Telemetry: Disabling telemetry stops data that’s being periodically sent from your computer from being sent.

5: Disabling file sharing: Disabling file sharing would make it much more difficult for someone to download and steal your personal files from your computer if connected to it.

6: Uninstalling Unused Applications: Uninstalling unused applications will help you avoid your system getting attacked through a vulnerability in the software you don’t use due to it not being updated regularly.

7: Disabling Guest account: Disabling the guest account in windows prevents users without the administrator password from getting access to admin privileges through windows 10 exploits.



8: Disabling Power Shell: Disabling Power Shell will help prevent users that gain access to your computer to use power shell based expoits.



9: Firewall Configuration: Blocking all incoming connections will prevent stuff that exploits the allowed connection settings to connect to you, even through allowed applications.



10: Remove Unnecessary Accounts: Removing unnecessary accounts prevents my system from being used by others, and also avoids loopholes in windows 10.

Sources: <https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-manage>

<https://www.tenforums.com/tutorials/68913-enable-disable-device-guard-windows-10-a.html>

<https://uit.stanford.edu/service/encryption/wholedisk/bitlocker>

<https://www.lifewire.com/disable-windows-remote-desktop-153337>

<https://www.easeus.com/partition-manager-software/fix-windows-10-microsoft-compatibility-telemetry-high-disk-usage.html>

<https://support.emsisoft.com/topic/28728-disable-powershell/>