10 Steps to Secure Window Secure Windows 10

1. Check that Windows Security is Setup Correctly

- Start → type **"Windows Security".** Verify that green checkmarks are on:
  - ✓ Virus & Threat Protection[1]
  - ✓ Account Protection
  - ✓ Firewall & network protection
  - ✓ App & Browser Control
  - ✓ Device Security

2. Enable Automatic Backups & Ransomware Detection

- If you have Office365 it includes 1TB of OneDrive Cloud Storage. OneDrive can automatically **Backup** your Documents, Photos, and Desktop. It also includes **Ransomware Detection** (and Protection in some cases), and **Versioning** which allows you to rollback all your files to a previous point in time.
  - Start → **"OneDrive"** → Open OneDrive and Right-Click your OneDrive folder in the left pane and choose Settings → Backup → Manage Backup → Enable backups for your Desktop, Photos, and Documents.
- Alternatively: Backblaze Cloud backup and SpiderOak One Backup are both good online backup providers. These do not have ransomware protection but do have versioning so you can rollback.

3. Encrypt your hard drive with BitLocker

- Control Panel → System and Security → Bitlocker Drive Encryption → Turn on Bitlocker (this requires a TPM module and Windows 10 Pro).
- Alternatively, some hard drives can be encrypted at the BIOS level.

[1] You don't need to buy an antivirus program, use the one that comes with Windows.

4. Enable System Restore

- Start → Control Panel → System & Security → System → Change Settings → System Protection → Configure → Turn on System Protection. Set the max usage to something like 10GB or 20GB. This will allow you to restore to a previous point in time should a change mess up Windows.

5. Enable Core Isolation

- Core Isolation prevents malicious programs from inserting bad code into high-security processes.
- Start → type **"Core Isolation"** → Enable Memory Integrity (this may not be compatible with older computers).

6. Install Few Apps and Remove Apps you Don't Use

- The fewer programs and apps installed the **smaller your attack surface area** for hackers.
- Start → Settings → Apps → Uninstall any programs you don't need or use.

7. Keep Software Updated

- Keep software on your computer updated. When a program prompts you to install updates do so. **Running outdated software and packages is a security risk.**

8. Use a Secure Browser

- **Chrome** – The most popular browser. Simple, secure, and fast.
- **Edge** – Secure browser with focus on compatibility and administration
- **Firefox** – Privacy Focused Browser
- **Brave** – Give users control of privacy and ads and publishers their fair share
- **Safari** – Browser designed for Mac OSX and iOS
- **Opera** – Built in VPN reduces online tracking

9. Use a Password Manager to manage your credentials

- **LastPass** is the most widely used password manager
- **KeePass** is an open source password manager that isn't cloud based
- **1Password** is another popular password manager
- **Password Safe** was written by cryptographer Bill Schneier

10. Enable Controlled Folder Access (Experts Only)

- Start → type **"Ransomware Protection"** → Enable Controlled Folder Access. **Note that you should not do this unless you know what you are doing.** This will prevent applications from accessing your documents and you'll have to whitelist applications one by one. It will cause lots of trouble if you use a lot of applications. It may be more trouble than it's worth unless you use a limited number of programs. However, it will stop most ransomware dead in its tracks.