Keeping Windows 10 Secure

John Allen, August 2017

Security in Windows 10 is different to previous Windows systems. It operates securely with its own built in protection mechanisms, including virus, malware, spyware, firewall and sandbox protection. Each monthly quality update, Microsoft adds another layer of security that "tracks emerging and changing trends in malware to make up-to-date systems safer in the face of changing and evolving threats"

Microsoft is continually adding more defences to Windows. In the Windows 10 "Fall update" in November, two new security features will be added that make similar features in 3rd party security applications redundant:

> ***Exploit protection*** - built in to Windows, it can operate whether Defender or a 3rd party antivirus is used. It detects exploits using behavioural techniques
>
> **Controlled folder access** (built in to Windows Defender) - this feature monitors the changes that apps make to files in certain protected folders such Documents, Pictures. You can specify which folders are protected and which apps are allowed to access your protected folders. If set up correctly, it would prevent rogue ransomware apps encrypting files

If you want to keep things simple, you don't need *any* 3rd party security products. You can feel comfortable that you have good protection, and just focus on using the computer, rather than spending time sorting out issues with 3rd party security apps.

This talk will take you on a tour of the Windows 10 Security settings, so that you know what is there. You don't need to change any settings. Again, if you want to keep things simple, just leave the default settings that Windows thinks is best.

Keep Windows updated, Use Microsoft Edge browser, stop using vulnerable apps, and don't use registry cleaners or "driver update" apps. Practice safe computing. Use strong passwords & 2 phase verification on your on-line accounts.

No amount of security applications will protect you 100%. The biggest security threat is who is sitting in the chair in front of the computer.

You will get varying advice about security for Windows 10: which is the best product etc. Some opinions may be valid for Windows 7 or earlier systems, but not necessarily for Windows 10, particularly the "Fall" update version coming in November.

Make sure Windows Updates are applied

This is the number 1 security priority. Most Windows updates install behind the scenes and you may not know they have occurred. Sometimes a computer restart is required. If you get a restart request, action it ASAP.

Don't attempt to interfere with Windows to delay or prevent updates occurring. You can manually check whenever you like*:*
Start > Settings > Update & security > Windows update > Check for updates.

You can also manually check for Defender updates whenever you like:
Start > Settings > Update & security > Windows Defender > Open Windows Defender Security Centre >
Virus & threat protection > Protection updates > Check for updates

You can also manually check for Defender updates whenever you like:
Start > Settings > Update & security > Windows Defender > Open Windows Defender Security Centre > Virus & threat protection >
Protection updates > Check for updates

Use Microsoft Store apps where possible

Microsoft Store apps are apps pre-installed with Windows 10, or apps that you obtain from the Windows Store.

Non-Store apps (called "Desktop apps") are pre-installed by the computer manufacturer (eg Security app, Acrobat reader, recovery app); installed from media such as CD, DVD, USB; or downloaded elsewhere from the internet.

Microsoft Store apps are subject to strict security quality control and only allowed in the Store if they are safe. Most Store apps are sandboxed, which means that they run in a protected cell. Any malware that gets in can't easily escape to the rest of the system. Edge browser and Office 365 are Store apps.

Edge is the only browser that will allow you to close a locked scam window, in other browsers you have to either shut down the computer or force close the browser using Task Manager.

As a general rule, unless you need additional functions, try to use Store apps such as *Photos*, *Groove Music*, *Films & TV*, *Mail*, *Office 365**. As for browsers, use *Microsoft Edge*. *Windows 10 S will only allow Store apps to run.*

Developers are creating Store app versions of popular Desktop apps. Microsoft Office 365, Adobe Photoshop Elements 15, and IrfanView, are examples of what is already available

** Technical note: Developers create Store app versions of their "Desktop" apps by "wrapping" them in a "Desktop Bridge container" using an application called Desktop App Converter.*

If you do use Desktop (ie non-Store) apps, the most unsafe ones are those downloaded elsewhere from the internet. Only download them from the developer's web site, there are many "doctored" versions out there that contain malware. Preferably, use apps from reputable developers. Research reviews first to see any reports of malware or nuisance-ware? During installation, untick any options to install additional software.

You can control the installation of "Desktop apps". Start > Settings > Apps > Apps & features > Installing apps. The setting *"Warn me before installing apps from outside the Store"* is useful if you are unsure of the difference between Store and Desktop apps

Checking your Windows Security Settings

Open the Windows Defender Security Centre

The Windows Defender Security Centre operates whether you use Defender antivirus or a third party antivirus. A 3rd party antivirus has to register itself with the Security Centre. Look at the Windows Defender Security icon:

- If it has a green tick, all is well
- If it has a yellow exclamation mark, something needs to be checked
- If it has a red x, you need to address a problem

Open the Windows Security Centre:
- Right click on the Defender icon > *Open*, or
- *Start > Settings > Update & security > Windows Defender > Open Windows Defender security centre*

Virus & threat protection – that will tell you if any action is required, or if a 3rd party antivirus application is protecting you. If you are using Defender antivirus, open *Virus & threat protection settings*, and ensure that *Real time protection* and *Cloud based protection* are *On.*

Device performance & health - it will indicate if there are any issues you need to address, otherwise it will say "No action needed"

App & Browser control:

"Check apps and files" – should be set to *Warn* or *Block*
"SmartScreen for Microsoft Edge" – should be set to *Warn* or *Block*
"SmartScreen for Windows Store apps" – should be set to *Warn*

Firewall & network protection - Make sure that either the "Windows firewall is on", orr if you have a 3rd party firewall, "No action needed".

Additional settings in the "Fall" Update

Exploit protection - Open the Windows Defender Security Centre > App & Browser Control > Exploit protection
(best to leave the default settings here!)

Controlled folder access –

Prevents "unfriendly" Apps from accessing your data folders such as Documents, Pictures, Music, Videos, or other folders that you choose. "Friendly" apps are Store apps, Office, etc., and apps that you allow. This feature would effectively stop ransomware encrypting your files. It is part of Windows Defender, so it is probably disabled if you use a 3rd party security app.

You can turn it on or off, add an app that is allowed to access your protected folders, or add additional folders to protect: Open the Windows Defender Security Centre > Virus & threat protection > Controlled folder access (example: allowing KeyPass to save files in Documents)

Check other security settings

Start > Settings > Privacy > General – set to your liking
Start > Settings > Privacy > Camera/Microphone – check to see which apps are allowed to use your camera and microphone, turn off any you don't want to give access.

Vulnerable 3rd party applications:

- **Adobe Flash player** – this vulnerable app is being phased out, but still may be used in some older web sites, for example, http://junglememory.com.
  Edge and Chrome will alert you if Flash is used (except for a few specific web sites).
  Avoid using web sites with Flash content. To totally disable Flash:
  Edge: *Settings & more* icon (three dots) > *Settings > View advanced settings*, turn off "Use Adobe Flash Player"
  Internet Explorer: *Tools > Manage Add-ons > Show* "All add-ons" > *Disable* "Shockwave Flash object
  Firefox: Press Alt button, *Tools > Add-ons >* Set Shockwave Flash to "Never activate"
  Chrome: n/a
- **Java** – also being phased out. Some web sites still use it such as some browser-based games and crosswords. *Uninstall Java if you have it installed.*
- **Apple Quicktime** – Apple stopped maintaining this some time ago. *If you have it, uninstall it*.
- **3rd party PDF readers** – You may have installed Adobe Acrobat Reader, or it may have been pre-installed on your system. ASUS, Acer and HP pre-install Foxit PDF Reader on their computers, it can cause problems with Windows Explorer in Windows 10. Edge browser opens PDF files. In the Windows 10 "Fall update", you can fill in PDF forms with Edge. Unless you want the additional features of these apps uninstall them. If you do use them, action any request to apply updates to keep them secure. To be sure, manually check for updates periodically - *Help > Check for updates*.

3rd Party web browsers

Windows Update will NOT keep 3rd party browsers secure. If you prefer to use Firefox or Chrome (or Opera, TOR or any other browsers), you need to make sure they are kept up-to-date. This should happen automatically, but you should check weekly anyway. To check for updates manually:

- **Google Chrome** – click the *Control* icon (three dots) > *Help > About Google Chrome*
- **Firefox** – Press Alt key (to see the menu) > *Help > About Firefox*

Some 3rd party security apps use their own browser for secure banking and shopping. These are updated by the App developer.

Be aware that you may see a false warning telling you to install an urgent Firefox or Chrome update, doing so could install malware. Ignore such requests.

Don't use any registry cleaners or "tune-up" applications

To name a few: *CCleaner, AVG TuneUp for PC, Avast Grime-Fighter, Wise Registry Cleaner, JetClean, Auslogics Registry Cleaner, Registry Mechanic, Advanced System Care, AML Registry Cleaner, Slim Cleaner, JV16 PowerToolsX, EasyCleaner*.

The Windows Registry is a database of settings for all hardware, software, and user preferences on your computer that controls how Windows interacts with your hardware and applications

These applications were useful in Windows 3.1, Windows 95, Windows 98, but are redundant since Windows XP.

They may irreparably damage your system, and the free versions may install unwanted toolbars and other applications on your computer.

Windows contains all the tools needed to keep your computer tuned, and the Creators version does this all automatically. Check the settings: *Start > Settings > System > Storage > Change how we free up space*. If you use a 3rd party browser, clean out its temporary internet files occasionally. The "Fall update" includes more options.

Microsoft warn not to use registry cleaners:
https://support.microsoft.com/en-au/help/2563254/microsoft-support-policy-for-the-use-of-registry-cleaning-utilities

Malwarebytes call these apps "digital snake oil". https://blog.malwarebytes.com/cybercrime/2015/06/digital-snake-oil/

For example, I ran CCleaner on Windows 10 and I then had zero search capability because CCleaner corrupted my user profile.

Don't use "driver update" apps

To name a few: *Ashampoo Driver Updater, Driver Booster, Free Driver Scout, Driver Pack Solution, Snappy Driver Installer, Slim Drivers, Driver Talent, Device Doctor, Driver Max, Drivers Cloud, Driver Reviver, Perfect Updater, Driver Scanner*, *Driver Detective, DriverUpdate*.

A Driver is Software/Information file in Windows that your computer needs to communicate with the "firmware" contained in a device. Every hardware component needs a driver to work properly. Drivers are specific to a particular operating system and system type (32 bit or 64 bit) - incorrect/faulty drivers can cause the component to be inoperable, or Windows to fail. *Windows 10 is the best driver update app!* Windows Update will automatically install the correct "signed" drivers for your devices, and keep them updated.

"If it ain't broke, don't fix it". When you have working drivers installed, leave them alone unless you are having problems with your device (eg WiFi dropping out, screen flicker on games, printer misbehaving, sound stuttering or failing).

If you suspect a driver needs updating:

1. Run Windows update which may find a new driver
2. Open the device in Device Manager and check for updates
3. Check the manufacturer's web site support page to see if there is a later driver you can install (make sure the model, operating system and type are correct)

If a device is malfunctioning, updating the driver may fix it, but occasionally a Firmware update is required. Firmware is built into the device itself, and operates independently of Windows. For more information, consult the device manual.

Driver update apps are unnecessary, rip-off, and dangerous! They were useful for Windows XP and earlier. Avoid them – you have no idea what they are installing on your computer. They may install unofficial or "doctored" drivers that cause problems or contain malware.

I installed DriverUpdate (supposedly a "Microsoft Partner") on an Acer netbook. It said that 1 driver needed updating. I was asked to purchase a monthly licence to update it, I refused. It installed a Startup app that nagged me every time I started the computer. I checked the Acer support web site, it said "Please run Windows Update to install the appropriate drivers".

If you have an old printer or other device that you want to connect to a Windows 10 computer, don't use the DVD/CD that came with it - just plug it in and see if Windows finds the driver. Maybe there are no drivers available for Windows 10. Visit the support page of the manufacturer's web site and see if a driver is available, or try installing an older driver in "compatibility mode".

Your on-line accounts

Use strong passwords for all your important accounts.
Use two step/factor authentication on all your important accounts so that you get a code in an email or SMS in order to login
In some cases you may only receive a code if you use a different computer, a different browser, or reset your browser, for example: Bank accounts, Paypal (the feature is called “Paypal Security Key”), Facebook, Gmail/Google account, Microsoft account, iCloud account (If you use a mail client to access your email, you will need to obtain a unique “app password” so the app can access your account).

BACKUP YOUR DATA !

- Backup your Documents, Pictures & Videos at least monthly
- Make two copies: one to a USB disk; the other to a different USB disk, or the Cloud (Google Drive, OneDrive, DropBox, Mega.NZ)
- Keep one of your backup disks disconnected so it is safe from a Ransomware attack
- With data backup I like to be able to see the actual files on the backup disk, not have them stored in zip files or in a format that requires a particular application to view or restore them
- Simple backup to a USB hard disk:
  Make a new folder on the hard disk, eg “Backup August 2017”
  Copy Documents, Paste to the new folder; repeat for Pictures, Videos
- Or use a Backup app like Personal Backup or SyncToy– John will give a separate session on using *Personal Backup* app

System Recovery

What happens if you have a catastrophic failure of Windows 10 or a hardware component? Windows 10 contains good system recovery features, but you should take the following minimum precautions to allow access, and because your data and applications may be destroyed in the recovery process:

- Have your data separately backed up
- Create a Recovery Drive (USB disk) - *Control Panel > Recovery*
- For any software apps you have installed, keep the original installation media, account details, and activation keys
- You can also create an image of your system using a 3rd party imaging application. I use Easus ToDo Backup

3rd Party Security products

Most new computers come with trial versions of a 3rd party security product such as Trend, McAfee, Norton, Kaspersky, Sophos, BitDefender. The computer manufacturer is paid to put it there. Your choices are:

1. Uninstall the product(s) and restart the computer. The built-in Windows 10 Defender security then activates automatically. You don’t need to install any other security app
2. Activate the pre-installed trial version - you must pay your annual subscription fee at the end of the trial otherwise you are left unprotected.
3. Uninstall the product and install a different 3rd party product(s) of your choice. There are many good 3rd party security products available, including freebies like AVG (owned by Avast), Avira, Avast.

In cases 2 or 3, the inbuilt *Windows Defender* antivirus disables itself.

All the above options give you real-time protection (see below)

The case against 3rd party security products

Using any 3rd party security application may add to the security, but the price is possible conflicting interaction issues with Windows, possible opening of new vulnerabilities, degradation of your PC’s performance, complicated settings, and false positives.

These 3rd party products put tentacles deep into the operating system, can interfere with Windows 10 built in security, and can cause issues such as Internet connectivity, crashes and hangs, issues with email, user profiles, Microsoft Office - more likely during or after Windows Feature Updates.

The new *Exploit* and *Folder Protection* features in the Windows 10 “Fall update” may further complicate the relationship between Windows and 3rd party security apps, and make some of their features redundant.

When a conflict issue occurs, it may not be obvious that the 3rd party application is the culprit. You may have to track down the issue by changing its settings, checking the support forum, temporarily disabling or uninstalling it. Of course, it may not be the culprit!

When the bi-annual Windows 10 feature upgrades occur, to ensure a smooth update if you have 3rd party security apps installed:
- Update your 3rd party security apps to the latest version (very important);

- then disable or temporarily uninstall any 3rd party security application to ensure a smooth system update (recommended);
- then allow Windows update to proceed;
- then enable or re-install your security app.

Using 3rd party security apps will impact on your PC's performance.

Some of these products replace the Windows firewall with their own firewall. The Windows 10 firewall is as good as any 3rd party firewall and does not need to be replaced.

5 minutes after installing McAfee LiveSafe, I got a comforting message saying that "since installing McAfee Livesafe [Firewall] it had blocked 8 incoming connections. T*he Windows Firewall would have blocked the same threats but not boasted about it. You can turn on logging on the Windows Firewall if you really want to see what it blocks.*

Whatever you do, run only ONE 3rd party antivirus, otherwise serious performance issues and conflicts can occur. For example, running Kaspersky and AVG, or McAfee and Avira, is a recipe for trouble. Malwarebytes Premium *is* designed to run alongside another antivirus, but both applications may need settings changes to co-exist

If you choose to use ANY 3rd party security product, be prepared to have to nurse the interaction between that product and Windows when some strange issue occurs. Join and follow the official on-line forum associated with the product so you can regularly monitor issues and seek assistance, eg:
https://forum.kaspersky.com/index.php?s=8c5f4eb7dce2347204a878a18d8dc605&showforum=4
https://support.avg.com/answers#!/feedtype=RECENT_REPLY&dc=AVG_Protection_v2&criteria=ALLQUESTIONS
https://community.mcafee.com/community/home/virusandspywareprotection
https://forums.malwarebytes.com/forum/41-malwarebytes-3

Real-time protection vs scanning

Your PC needs **real-time** protection to help protect it from being infected, that means in simple terms that web sites, files, and other activities are checked before being opened, thereby preventing infection.

Malware **scanning** won't stop your PC being infected, but may detect existing malware infections and clean them.

Defender, and all 3rd party antivirus apps include both Real-time protection and scanning features. Malwarebytes Premium adds additional real-time protection. Other apps such as: Malwarebytes free, HitmanPro.Alert, Zemana, SuperAntispyware are also useful as secondary scanners, and for cleaning up an infected computer

What security products do I currently use?

Windows Defender and Malwarebytes as an occasional scanner

Further information

Mr Robert O'Callahan, a highly respected NZ engineer who used to work on Firefox, and recipient of the Mozilla Distinguished Engineer Award 2013 has written a paper explaining why just using Windows Defender is recommended.
Ref: http://robert.ocallahan.org/2017/01/disable-your-antivirus-software-except.html

Settings documented in this paper relate to Windows 10 version 1703 (Creators version) and the "Fall update" due in November

John's Charcoalition web site
www.coastwatchers.org.au/charcoalition/index.html