Microsoft Windows certainly ranks as the world's most popular consumer operating system, but also scores as the highest target for malware, security attacks and attacks. The purpose of this post is to understand the methods to make Windows 10 safer and more secure.

The majority of new malware targets the known (past) vulnerabilities of Windows, and looks at some of the insecure (poor) user practices we need become aware of.

With the latest Windows 10 (version 1803 or greater), you no longer need buy an anti-virus, firewall or anti-malware suite. Windows 10 (latest), has some very good security already included and operative. More than ever in history, Microsoft is dedicated to providing Windows 10 as a secure operating systems, along with secure apps, such as Microsoft Edge.

Windows Privacy settings

Windows sends information about events on your computer to Microsoft and also to other servers which can be considered to violate your personal privacy. To limit (but not entirely remove) this information leak, we will investigate some of the better Windows privacy configuration options you can choose. The steps will depend if your installing a fresh copy of Windows on a computer or you already have Windows installed.

> Windows 10, by default, has permission to report a huge amount of data back to Microsoft. By clicking through “Express Settings” during installation, you allow Windows 10 to gather up your contacts, calendar details, text and touch input, location data, and a whole lot more. The OS then sends it all back to Microsoft so that it can be used for personalisation and targeted ads.

Better privacy-protection options when installing Windows

During the installation of Windows 10 one of the default choices is to accept **Express Settings**; this section has a large number of “invasive” Microsoft default options to send your personal data to Microsoft and also to some advertising partners.

Windows 10 Installation – Customize Settings
Suggestion: Instead of accepting **Express Settings**, select **Customise settings** – at the left – bottom.

You should make your own personal choices of the options below based on your own preferences and comfort. The chosen options outlined below are simply based on my own suggestion regarding some sensible privacy and security. Your choices may vary from my own.

On the **Customise Settings** section – as shown below, if you select on an option, it will toggle to

Windows 10 Install Customize Settings Privacy #1
Select to move to the next **Customise Settings** section.

On the next **Customise Settings** setting I suggest that you leave **Use SmartScreen online service to help protect against malicious content and downloads in sites loaded by Windows browsers and Store apps** enabled as this does enhance security. Howsoever, for the remaining options I suggest that you click and thus change them to values.

Windows 10 Install Customize Settings Privacy #2
Select to continue with the Windows installation.

Better privacy-protection options if Windows is already installed

If the case of an existing installed Windows 10, you can select the privacy options as shown below:

Select **Settings** through the main Windows Start menu, as shown below:

Windows 10 Start Menu – Settings

Select **Privacy** from the **Settings** section.

Windows Settings Privacy

Using the following tabs, configure your preferred settings to enhance your privacy – or use my suggestions.

General tab (privacy)

Select “**Off**” to disable all the options below to limit the data collected by third parties.

Windows 10 Settings General – Privacy Options

Location tab (privacy)

Select the button under **Location** to turn thist **off**. This option simply prevents third parties from collecting your location inforamtion.

Windows Settings Location Off

Now further down the same page you will see a **Location history** section. Now select **Clear** to erase your device location history.

Windows Settings Clear Location History

Now further down the same page you will find the section to configure the apps that have access to your location. Choose the access (on or off) of these apps to use your location. Some recommendations are made for you on items such as “**Cortana**” and “**Microsoft Edge**“.

Windows Choose apps to use Location

Camera tab (privacy)

Select “**Off**” under “**Allow apps to access your camera**“.

Windows Settings – Privacy – Camera

Alternatively, you can restrict certain apps from accessing your camera, selectively turn “**off**” a respective app.

Microphone tab (privacy)

Select “Off” under “**Allow apps to access your microphone**”

Windows Settings Privacy Microphone

Alternatively, you can restrict certain apps from accessing your microphone, selectively turn “**off**” a respective app.

Speech, inking, & typing tab (privacy)

Select to turn “**Off**” the selection under “**Getting to know you**“. This will effectively prevent Microsoft from collecting information such as your contacts, typing history, calendar events, speech and handwriting patterns.

Windows Settings Inking & Typing

Account info tab (privacy)

Select to turn “**Off**” the selection under “**Allow apps to access your account info**” to disable apps from accessing your account information.

Windows Setting Account Info access

Contacts tab (privacy)

Select to turn “**Off**” the selection under “**Allow apps to access your contacts**” to disable apps from accessing your contacts.

Alternatively, you can restrict certain apps from accessing your contacts, selectively turn “**off**” a respective app.

Windows Settings Privacy Contacts access

Calendar tab (privacy)

Select to turn “**Off**” the selection under “**Allow apps to access your calendar**” to disable apps from accessing your calendar.

Alternatively, you can restrict certain apps from accessing your calendar, selectively turn “**off**” a respective app.

Windows Settings Privacy Calendar access

Call History tab (privacy)

Select to turn “**Off**” the selection under “**Allow apps to access your call history**” to disable apps from accessing your calendar.

Alternatively, you can restrict certain apps from accessing your call history, selectively turn “**off**” a respective app.

Windows Settings Privacy Call History access

Email tab (privacy)

Select to turn “**Off**” the selection under “**Allow apps to access your email**” to disable apps from accessing your email.

Alternatively, you can restrict certain apps from accessing your email, selectively turn “**off**” a respective app.

Windows Settings Privacy eMail access

Messaging tab (privacy)

Select to turn “**Off**” the selection under “**Allow apps to read or send messages**” to disable apps from accessing your messaging.

Alternatively, you can restrict certain apps from accessing your messaging, selectively turn “**off**” a respective app.

Windows Settings Privacy Messaging access

Radios tab (privacy)

Select to turn “**Off**” the selection under “**Allow apps to control device radios**” to disable apps from accessing your Radios.

Alternatively, you can restrict certain apps (if any show) from accessing your radios, selectively turn “**off**” a respective app.

Windows Settings Privacy Radios access

Other devices tab (privacy)

Select to turn “**Off**” the selection under “**Communicate with unpaired devices**” to disable apps from accessing any unpaired devices.

Alternatively, you can allow (or dis-allow) certain trusted devices that are already connected.

Windows Settings Privacy Other Devices access

Feedback & diagnostics tab (privacy)

In this section you choose the feedback frequency and diagnostic data sent to Microsoft. I recommend using **“Never”** be asked for feedback and sending only “**Basic**“ diagnostic information. However, if you are a member with Microsoft Insider (early Windows releases ring) then leave the choices here alone.

Windows Settings Privacy Feedback & Diagnostic

Background apps (privacy)

In this section choose the apps you wish to allow as running in the background (receiving information, sending notifications, and staying up-to-date). I would recommend you switching of any that you deem to be not important. Skype and Windows

Security are tow that I would leave enabled. Possibly consider allowing Mail and Calendar if you like alerts from email or reminders.

Windows Settings Privacy Background Apps access

User Account Security : Password

Password protection your user accounts and having separate user accounts for each user accessing the computer are one of the very basic requirements for better security.

Check if your Windows account is already password protected

Lock your computer screen by using + **L**. (screen lock short-cut keys). If your user account has a password then you will be asked to enter it here. If your user account does not have a password then you will allowed to sign in without a password.

On most keyboards the Windows key is a key located between the **Ctrl** and **Alt** keys, it will normally have have a or icon label.

Windows 10 Sign In Lock Screen

Add a password to a Windows User account

Tap the Windows key to open the Windows Start menu then click to open the **Settings** section of Windows.

Choose the **Accounts** section

Windows 10 Settings Accounts

Now select **Sign-in options** from the left side.

Windows Settings Account add Password or PIN
Select **ADD** below password.

Use a PIN: Note that optionally you can use a PIN. The use of a PIN allows a faster login as only the numbers are required. The minimum PIN length is four digits (0–9 only), it can be longer. Generally, Passwords are sometimes easy to guess as they are often things such as pet or favorite celebrity. PIN numbers are more obscure and harder to guess, but can also be prone to the ‘convenience’ factor if a mobile number or date of birth is used. This is how it that option appears:

Windows Settings Accounts Create PIN
Enter a new password into **New password** and **Reenter password**. Use the “**Password hint**” field carefully as to not reveal too much information about the password.

Windows Settings Accounts Create Password
Now Select **Next** to apply the new password.

Adding a new Windows user account to Windows

To create a new Windows user account (or a guest account) the steps are:

Select **Accounts** through the Windows **Start** > **Settings** menu.

Windows 10 Settings Accounts
Select the "**Family & other users"** on the left side.

Windows Settings Account New User
Select the plus sign next to **"Add someone else to this PC"** under the "**Other users**".

Now select the "**I don't have this person's sign-in information"** choice on the "**How will this person sign in**" section.

Create new Account without Sign-in info
Now select the **"Add a user without a Microsoft account"** option on the "**Let's create your account**" section.

Windows new account without a Microsoft Account
Now enter the **user name** for this new account under the "**Who's going to use this PC?**" section.

Windows Settings Create an account
Enter a **password** for this new account under the "**Make it secure**" section.

Re-enter the password.

Use the "**Password hint**" field carefully as to not reveal too much information about the password.

Select **Next** to complete the new account.

You will see the new account in the **"Family & other users"** section of Account Settings.

Setup a Screen Lock

A screen lock can deter unwanted guests from physically accessing your computer. You can either manually lock access to your machine if you step away from the computer or have the screen lock automatically lock after a period of inactivity.

Setup a automatic timer screen lock when your computer is inactive

With this option your computer can automatically lock itself after a selected period of inactivity.

Use the Start button and enter a search for "**Change screen saver**" without the quotes.

Choose the section “**On resume, display logon screen**” to activate the screen lock timeout.

Now enter the number of minutes of inactivity to wait before automatically locking the screen. Usually a short timeout period is wise.

Windows Settings Screen Saver Settings Lock
Select **OK** to apply the new screen saver settings.

Security

When you use Windows 10 for the first time, Windows Security is enabled and actively protecting your computer by automatically scanning for malicious software, viruses, and security threats. Windows 10 Security uses real-time protection to scan every item you download or run.

Updates

Windows 10 automatically downloads and installs Windows updates for you. If you have had your Windows 10 machine turned off for sometime, it is important to manually check for updates at a early opportunity. To do so use the Windows key and then , now find and open the section “**Update & Security**“. Now choose the “**Check for updates**“.

Windows Settings Update & Security
Wait while the check is done. Follow through to install any updates that appear in the result.

Windows Settings Checking for Updates installing

Windows Firewall

The Windows firewall is normally active at all times. This is intentional to protect your operating system from outside unauthorised access to your computer through the Internet.

To check that your Windows firewall is on, do the following:

Use the Windows key and then , now find and open the section “**Update & Security**“. Now choose the “**Windows Security**“.

Windows Open Windows Security

Windows SmartScreen

SmartScreen is security feature in Windows 10 which is designed to protect users from malware and phishing attacks by scanning URLs that you access against a known (and regularly updated) **blacklist** of websites containing **threats**.

To access SmartScreen in Windows 10:

Use the Windows key and then , now in the search window at the top type “**smart**” **–** without the quotes.

You will see s result as shown below:

Windows Settings SmartScreen access

Now choose “**App & browser control**“. You will see the settings as per below:

Windows Settings SmartScreen App & browser

If you scroll down the “**App & browser control**” page you will see the option for “**Install Windows Defender Application Guard**“. You can read more about that protection option here.

Windows Settings SmartScreen Application Guard

Windows Defender

Windows Defender is a defensive software suite designed to detect malware and security threats and thereby protect your computer.

With the latest Windows 10 version April 1803 update, Defender has now reached the point where it offers some very good protection. You can read more about that feature here.

Windows Settings Windows Defender

To scan your computer for malware with Windows Defender, select the “**Quick Scan**” above:

Windows Virus & threat protection Quick Scan

Use the Windows key and then , now find and open the section “**Update & Security**“. Now choose the “**Windows Security**” option on the left.

Windows Settings Windows Security at a glance

The above stats windows offers a excellent summary on how your computer is being protected.

You should normally see a green ticks against most of the items – as is shown above.

Windows 10 will automatically download new definitions regularly to protect your computer.

You can easily see when the last definitions were updated by opening the section “**Update & Security**” then choose the “**Windows Security**” option on the left. Now open the “**Open Windows Security**” section.

Now open the “**Virus & threat protection**” sections:

Windows Virus & threat protection Updates Check

The status for “**Virus & threat protection updates**” section shows that “**protection definitions are up to date**“, and the last update was on 19/10/2018 at 12:59AM

The “**Current threats**” section (above) area allows you to:

- Initiate a manual Scan for threats on your device.
- See any threats currently on your device.
- See threats that have been quarantined previously.
- See items identified as a threat that you have allowed to run on your device.
- See the last time a scan was run on your device and how many files were scanned.
- Initiate a specific type of scan.

Quick scan is useful when you to perform a fast scan on your files and folders. If you are required to run a more comprehensive type of scan, you will be notified after “quick scan” is done.

Ransomware Protection

The latest Windows 10 now includes “**Controlled folder access**” which can prevent “ransomwear” from making your data hostage and can prevent unwanted changes to your files:

To access this section, Use the Windows key and then , now find and open the section “**Update & Security**“. Now choose the “**Windows Security**“.

Now open “**Virus & threat protection**” scroll down until you find the section “**Ransomware protection**” as shown below:

Windows Virus & threat protection Ransomware
Now if you select the section “**Manage ransomware protection**” you will see the following:

Windows Ransomware Controlled Folder list enabled
The above image does show that I have enabled “**ransomware protection**” for “**Controlled folder access**“**.** Now I can select the folder to protect by selecting “**Protected folders**” as can be seen below:

Windows Ransomware Controlled Folder list
When the “**ransomware protection**” for “**Controlled folder access**” is enabled, it intelligently tracks access executable files, scripts, and DLL’s trying to make changes within the protected folders. If the access is seen as malicious, or it’s not recognized, a real-time block occurs, and you will receive a notification of the suspicious activity.

As a default, the ransomware protection guards your Documents, Pictures, Videos, Music, Desktop, and Favorites folders. You cannot change that list, however you can a new drive or folder to the list to be protected to that list.

Allowing specific apps

Controlled folder access should be smart enough to detect which apps can safely access your files, but it the case an app you trust is blocked, you’ll need to allow the app manually.

Use the Windows key and then , now find and open the section “**Update & Security**“. Now choose the “**Windows Security**“.

Now open “**Virus & threat protection**” scroll down until you find the section “**Ransomware protection**” as shown below:

Windows Ransomware Controlled Folder access
Select the section "**Allow an app through Controlled folder access**". You will see this:

Windows Virus & threat protection Ransomware Whitelist apps
Choose to allow (white-list) an app by "**Browse all apps**" or "**Recently blocked apps**".

Note that this is a unique security feature of the Windows Defender Exploit Guard and it is only if you use the Windows 10 Defender Anti-virus! This option is **not available** if you choose another third-party antivirus package. See this why Windows 10 is good enough for your protection.

Was this page helpful?

Related Posts

Windows Update

*Some settings are managed by your organization
View configured update policies

Updates failed

There were problems installing some updates, but we'll try again later. If you keep seeing this and want to search the web or contact support for information, this may help:

2018-07 Cumulative Update for Windows 10 Version 1803 for x64-based Systems (KB4345421) - Error 0xca00a000

Repair, Reset & Troubleshoot Windows Update errors in Windows 10

The Windows 10 Update service enables the operating system to download and install the latest updates, along with bug fixes, ...

READ MORE

The operation of Automatic Maintenance in Windows 10

With Windows 10, automatic maintenance runs in the background whenever the computer becomes idle, including when you sleep, as long ...

READ MORE

Windows 10 Home versus Windows 10 Pro: What is the Difference?

Most new computers will come with Windows 10 Home, however Windows 10 Professional includes a couple of features that may ...

READ MORE

Sitemap
Location Map
Privacy Policy

- Computer Repairs & Support | Victor Harbor