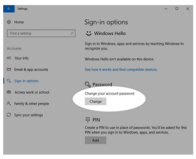
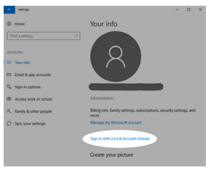
HOW TO PROTECT PRIVACY ON WINDOWS 10

1 Use a password rather than a PIN for local accounts.

Whether you use a local account or Microsoft account, make sure you use a strong, alphanumeric password.



2 You don't have to link your PC with a Microsoft account.

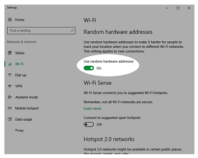


You can create a local account instead. This avoids sharing data about your account, although you lose the ability to share data across devices.

How: Settings > Accounts > Sign in with a local account instead

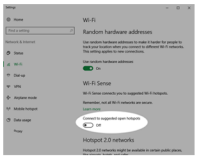
3 Randomize your hardware address on WiFi.

Enabling random hardware addresses makes you less prone to tracking across different WiFi networks. Note that not all devices support this.



How: Settings > Network & Internet > Wi-Fi

4 Don't automatically connect to open WiFi networks.

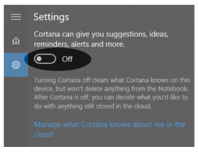


Windows 10 can connect to suggested open WiFi hotspots automatically. Disable this setting to give you more control over your network connections.

How: Settings > Network & Internet > Wi-Fi

5 Disable Cortana to keep voice data private.

Using Cortana, the voice-controlled assistant, sends commands back to Microsoft as well as data about your files for local search. Disabling Cortana is more private but you lose voice-control functionality.



How: Settings > Cortana

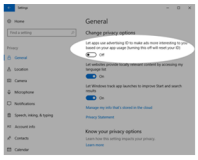
6 Watch out for system updates changing your privacy settings.

System updates are enabled by default which could revert your settings or add new ones, granting more access to parts of your system. Go back and check your settings after each major update, including looking for new items.

Most privacy settings on Windows 10 are accessible in the Privacy area of Settings. We recommend looking through each section in detail, though here are the main settings to look out for.

7 Don't share your advertising ID with apps on your system.

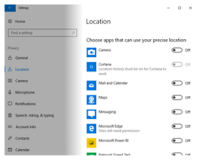
Disabling this also resets your advertising ID.



How: Settings > Privacy > General

8 Control which apps and services have access to your location.

You could also disable this entirely if not needed.



How: Settings > Privacy > Location

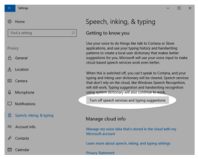
9 Control which apps can access sensitive data.

You can block access to features such as camera, microphone, contacts, calendar and call history.

How: Settings > Privacy > Camera/Microphone/Contacts/ Calendar/Call history

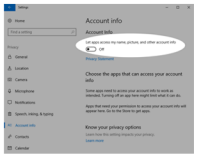
10 Stop your speaking and typing being sent to the cloud.

Note that this needs to be enabled to be able to speak to Cortana.



How: Settings > Privacy > Speech, Inking, & Typing

11 Keep your account info private.

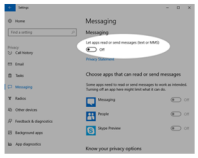


Decide which apps, if any, should have access to your account details such as your name and picture.

How: Settings > Privacy > Account info

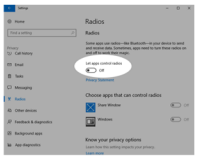
12 Restrict the apps that can send or receive messages.

Electronic communications often contain sensitive data, so consider which apps really need access to your email, text or MMS messages.



How: Settings > Privacy > Email/Messaging

13 Decide whether apps can control radios such as Bluetooth.

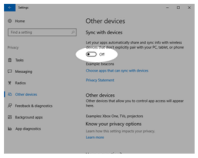


Note that turning this off doesn't disable Bluetooth, it just prevents apps from being able to control it.

How: Settings > Privacy > Radios

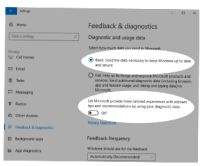
14 Control apps' ability to sync with non-pairing devices.

Examples of such devices include beacons that transmit advertising information to devices in close proximity, such as in retail outlets.



How: Settings > Privacy > Other devices

15 Limit the feedback and usage data that is sent to Microsoft.



Note that in "Feedback & diagnostics" only "Basic" is available—there's no "Disable." We recommend also turning off the tailored tips based on your data.

How: Settings > Privacy > Feedback & diagnostics

Congratulations! You've just taken a big step to increasing privacy and protecting the data on your Windows 10 system.

https://spreadprivacy.com/windows-10-privacy-tips