

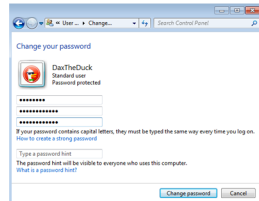


HOW TO PROTECT PRIVACY ON WINDOWS 7

1 Ensure you use a password to protect your user account.

It goes without saying that this should be a strong, lengthy password.

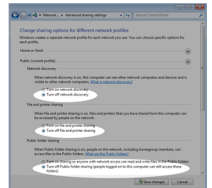
How: Control Panel > User Accounts & Family Safety > User Accounts > Change Your Password



7 Check the sharing options for your account profiles.

You can control individual services such as network discovery, file and printer sharing, etc.

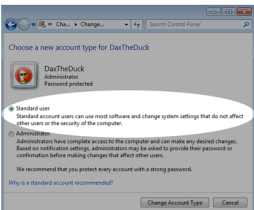
How: Control Panel > Network & Internet > Network & Sharing Center > Advanced sharing settings



2 Don't use an Administrator account by default.

For everyday computing, switch to a separate Standard user account to protect against malware doing system-wide damage.

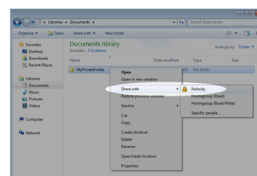
How: Control Panel > User Accounts & Family Safety > User Accounts > Change Your Account Type



8 Keep certain files and folders private.

If you're on a network, specify which files and folders are not shared with others.

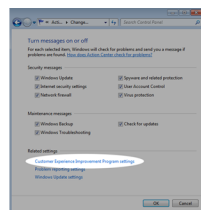
How: File explorer > [right-click on file/folder] > Share with > Nobody



3 Opt out of the Customer Experience Improvement Program.

This should also prevent the installation of some files related to upgrading to Windows 10.

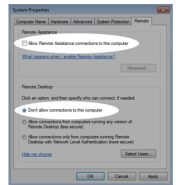
How: Control Panel > System & Security > Action Center > Change Action Center settings > Customer Experience Improvement Program settings



9 Turn off Remote Assistance and Remote Desktop.

Don't allow these remote connections to your computer, unless you're sure you need it.

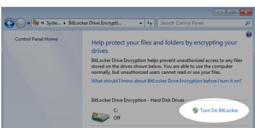
How: Control Panel > System & Security > System > Remote



4 Easily encrypt your PC with the built-in BitLocker.

Turn BitLocker on to make your files unreadable if someone else gets hold of your computer while powered off or locked.

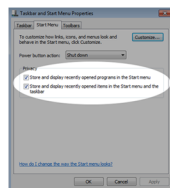
How: Control Panel > System & Security > BitLocker Drive Encryption



5 Stop recently opened programs and files being displayed in the Start menu.

This is particularly relevant if you're using a shared computer.

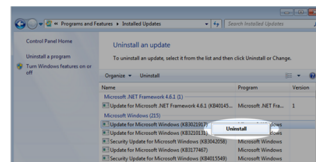
How: Start Menu > [right-click] > Properties



Data-collecting System Updates

10 Remove tracking and data collection updates.

There are several system updates that add tracking and diagnostic capabilities to your PC, some to prepare for an upgrade to Windows 10. If you don't have automatic updates enabled, you can refuse or remove these specific updates:



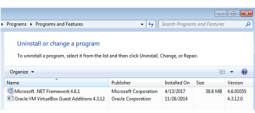
- KB3015249—Adds telemetry capabilities
- KB3021917—Prepares for upgrade to Windows 10
- KB3022345—Installs diagnostic tracking service
- KB3035583—Prepares for upgrade to Windows 10
- KB3044374—Prepares for upgrade to Windows 10
- KB3050267—Prepares for upgrade to Windows 10
- KB3068708—Introduces the Diagnostics and Telemetry tracking service
- KB3075249—Adds telemetry points to the User Account Control
- KB3080149—Updates the Diagnostics and Telemetry tracking service

How: Control Panel > Programs > Programs and Features > Installed Updates > [right-click to remove]

6 Review your installed programs.

To further reduce your exposure to privacy leaks, take a few moments to check which programs are installed that you no longer use, or that were pre-installed and are unneeded.

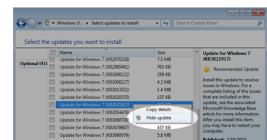
How: Control Panel > Programs > Programs & Features



11 Prevent tracking and data collection updates being installed.

You can prevent these updates from being installed in future by hiding them from the update system.

How: Control Panel > System & Security > Windows Update > Available updates > [right-click to hide]



Congratulations! You've just taken a big step to increasing privacy and protecting the data on your Windows 7 system.

<https://spreadprivacy.com/windows-7-privacy-tips>