



## Microsoft Windows - Safe and secure

1. Ensure the built-in Windows 8 or Windows 10 firewall is turned on. A firewall protects your computer or network from malicious or unnecessary network traffic.
2. Turn on automatic software updates in Windows. This will ensure that the Operating System (OS) is kept up to date with all security and functional changes. Most non-Microsoft apps come with options to auto-update too.
3. Windows 8 and 10 have built-in anti-virus software. If you don't use a 3rd party product then make sure the Windows anti-virus is activated and kept up to date.
4. Choose, use and protect your passwords carefully, use a different one for every online account in case one or more get hacked.
5. Don't click on links in emails, posts, tweets or texts and don't open attachments if the source isn't 100% known and trustworthy, or it seems strange that you'd be receiving them.
6. Avoid pirated software and other digital material. Streaming or downloading movies, music, books, applications etc. that don't come from legitimate sources is not only illegal but could pose a security threat to your computer as they may allow viruses or other malicious software (malware) to infect your system.
7. Don't plug in USB or other external devices unless you own them as they could contain viruses or malware.
8. Make sure your home WiFi is set up to use a secure network protocol with a strong password.