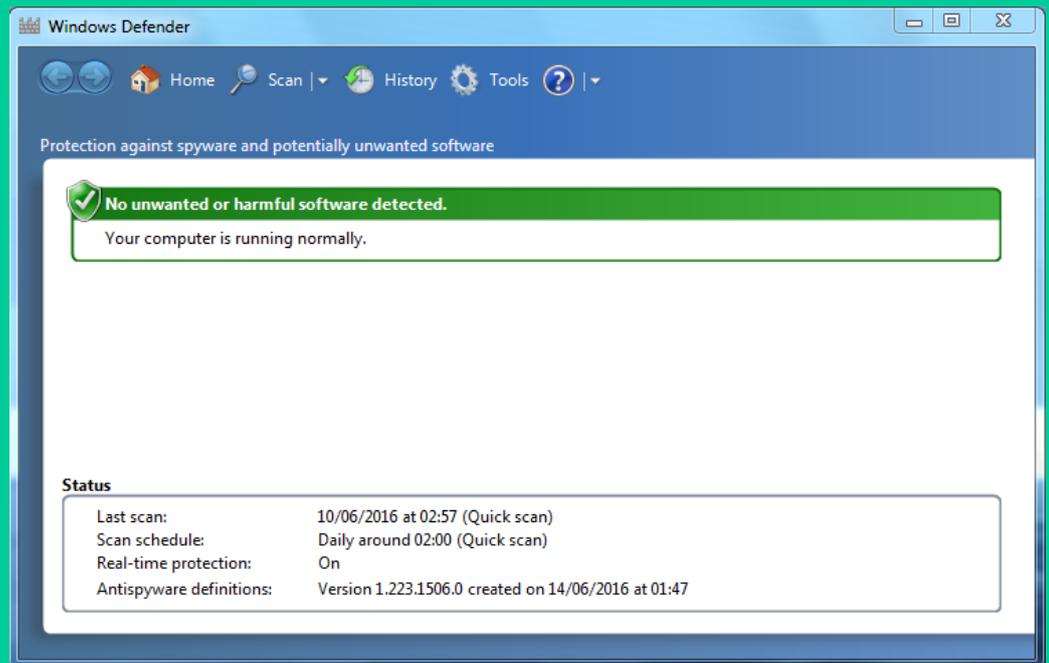


ANTI-VIRUS... THAT'S IMPORTANT RIGHT?

ANTI-VIRUS programs are a very important aspect of computer security. They provide an invaluable line of defence by scanning potentially malicious files which are about to be or have just been downloaded. If any files are deemed to be malicious, the Anti-Virus software will try to quarantine and delete these files.

VIRUSES are a type of malware and are typically created by a computer hacker. Hackers employ a variety of techniques to try and execute viruses on your computer. Potential effects include file theft and deletion, downloading additional malware and corruption of hardware and removable storage.



WINDOWS 7, 8 and 10 include Windows Defender – a basic albeit useful anti-virus scanner that is a part of the operating system. It is active by default and a screenshot of its operation in Windows 10 is shown above. MAC users do not have anti-virus by default however free anti-virus for MAC's is available from Avast: www.avast.com/free-mac-security

DON'T rely purely on your anti-virus software. It provides an invaluable layer of defence however it is not fool-proof and can be ineffective against newer types of viruses. Bearing other computer security principles in mind – avoiding clicking on dangerous links, not accessing unknown pen drives and general internet safety – will also help.

AS WELL AS ensuring Windows Defender is functioning correctly, you should undoubtedly invest in anti-virus software from a 3rd party. Windows Defender provides a good baseline however it lacks the overall effectiveness of similar products – investing in even a free anti-virus program will assist with this.

REMEMBER anti-virus software should be your last line of defence and therefore it is a necessity. However, optimal computer security is about making as many layers of your system as secure as possible. There is no such thing as perfect security or perfect anti-virus.