



Factsheet 1—Secure computing checklist

By applying the following steps you can significantly improve your online security and, in particular, prevent malware from compromising your computer's security and potentially stealing your personal information or harming your files.

To minimise the risks as much as possible, regard the list as a complete set and do not simply follow two or three of the steps.

1. Use only supported operating systems

Vendors, including Microsoft, stop supporting operating systems that become dated. New versions offer improved security. Third-party vendors, which make application software for these operating systems, also stop support of older versions.

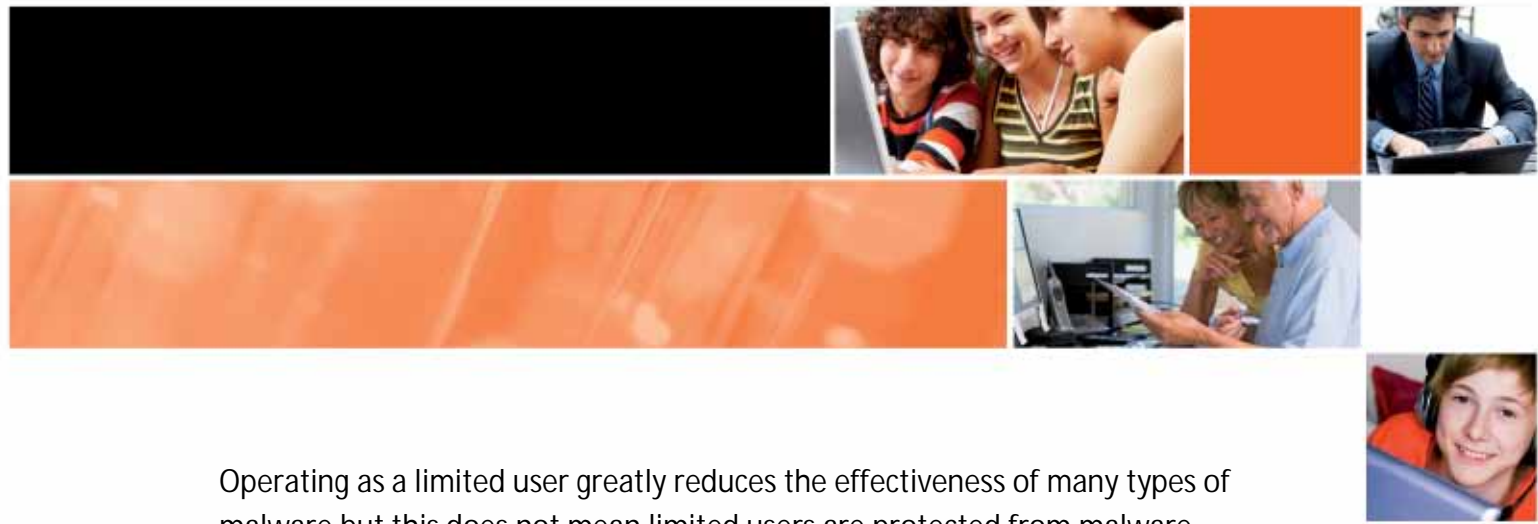
2. Enable automatic updates of your operating system

Automatic updates install small corrections to the operating system. These corrections are known as patches and include security and functionality improvements. When you enable the automatic installation of the fixes, you reduce the chance of exposure to security threats.

For further information, see [Factsheet 2](#)—Setting up automatic updates in Windows XP; [Factsheet 22](#)—Setting automatic updates for Windows Vista; [Factsheet 23](#)—Setting up automatic updates for Windows 7; or [Factsheet 24](#)—Setting automatic updates for Apple Mac OS X.

3. Enable a limited-rights account for each user and use it for routine online activities such as browsing the web and reading email

It is important to use a limited account for daily tasks as many malware authors depend on users running administrator (or privileged user) default accounts.



Operating as a limited user greatly reduces the effectiveness of many types of malware but this does not mean limited users are protected from malware completely. See [Factsheet 3](#)—Setting up a limited user account in Windows XP.

4. Install and update security software that provides functionality for antivirus and anti-spyware software and a personal firewall.

These products help prevent computers from infection by malware. Make sure that they are configured to update automatically. Do not install more than one product that duplicates any of these functions. Either install a product that combines these functions, or install separate products for each of these functions. For example, install a combined antivirus and anti-spyware product and a separate firewall product. See [Factsheet 18](#)—Free security software for non-commercial use.

5. If using broadband, turn your computer off when not in use.

See [Factsheet 16](#)—Securely configuring your broadband modem/router.

6. Secure your email software

One method of compromising your computer is via email. If you secure your email software, then you greatly reduce your chances of being compromised.

7. Secure your web browser

Another risk to your computer is during web browsing. If you secure your web browser, you can reduce the chance of your computer being compromised.

8. Do not click on links or open attachments in spam email or email that is otherwise suspicious.