

STAY SMART ONLINE ALERT SERVICE

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 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 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 being exposed to security threats. See Factsheet 2

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

The importance of using a limited account for daily tasks lies in the fact that many malware authors depend on the default that users are running as Administrators, also known as privileged users. Operating as a limited user greatly reduces the

effectiveness of many types of malware but does not mean limited users are protected from malware completely. See Factsheet 3.

4. Install and update Antivirus, Antispyware and Personal Firewall Software

These products help prevent computers from being infected by malware. Make sure that they are configured to update automatically.

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

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 way to compromise your computer is via the web. If you secure your web browser then you can reduce the chance of your computer being compromised.

8. Don't click on links or open attachments in spam email, or email that is otherwise suspicious.