



## Factsheet 18 – Free security software (for Microsoft Windows XP and Windows Vista)

It is a common misconception that to create a safe computing environment on a Microsoft Windows XP or Microsoft Windows Vista<sup>1</sup> based home computer, it is necessary to spend a lot of money purchasing security software.

There are a variety of excellent reputable free tools and packages available for download that can help you secure your computer, as well as a number of web-based services which can be used for the purposes of detection, disinfection and checking to see that you have up-to-date versions of your software.

This factsheet contains information regarding a number of these freely available tools and packages, web-based services, and also details a number of features contained within Microsoft Windows itself, all of which can help to reduce the risk of your computer being compromised. The four types of software which will be outlined in this factsheet and can be obtained freely for non-commercial use are:

- Anti-virus and anti-spyware
- Firewall
- Anti-spam
- Web-based online scanning services

**Some of the software mentioned in this factsheet is free for anyone to use, but in most cases the software is only free for non-commercial use, which means it is designed for home users and not for any commercial business entity. Please check the terms and conditions of use before installing and using this software.**

<sup>1</sup> Some of these products may be suitable for Microsoft Windows 7 and other operating systems. Check the system requirements first.



## Anti-virus and anti-spyware software

There are subtle but important differences between products which have anti-virus and anti-spyware functionality. Traditionally, this functionality was contained in separate products and it was necessary to install one anti-virus and one anti-spyware product. But this situation is changing and now many products combine anti-virus and anti-spyware functionality, inter alia, into a single product.

Computer software with anti-virus (AV) functionality is used to identify and remove not only computer viruses, but also many other types of harmful computer software, which are generally referred to as malware (or malicious software).

Installing software with anti-virus functionality is absolutely essential in today's computing environment and there are a number of products available for non-commercial use which will help to protect your personal computer. These products may not have as many features as commercial products, but they provide a basic level of protection that is necessary at all times, whether your computer is connected to the Internet or not. There are numerous products with anti-virus functionality available, but some of the more popular products which are free for non-commercial use are:

Package	Link	Functionality <sup>2</sup>
Avira AntiVir	<a href="http://www.free-av.com/en/download/1/avira_antivir_personal_free_antivirus.html">http://www.free-av.com/en/download/1/avira_antivir_personal_free_antivirus.html</a>	Combined anti-virus and anti-spyware functionality. May need to enable these options <sup>3</sup>
avast! Home Edition	<a href="http://www.avast.com/eng/download-avast-home.html">http://www.avast.com/eng/download-avast-home.html</a>	Combined anti-virus and anti-spyware
AVG Free	<a href="http://www.avgfree.com.au/">http://www.avgfree.com.au/</a>	Combined anti-virus and anti-spyware

<sup>2</sup> If the product combines anti-virus and anti-spyware functionality do not install another anti-virus or anti-spyware product on the computer at the same time.

<sup>3</sup> [http://www.free-av.com/documents/products/pdf/en/man\\_avira\\_antivir-personal\\_en.pdf](http://www.free-av.com/documents/products/pdf/en/man_avira_antivir-personal_en.pdf)



Microsoft Security Essentials	<a href="http://www.microsoft.com/Security_Essentials/">http://www.microsoft.com/Security_Essentials/</a>	Combined anti-virus and anti-spyware
-------------------------------	---	--------------------------------------

These programs check for updates on a daily basis when your computer is connected to the internet, or as scheduled. It is important that these regular updates are received to ensure that you are protected as many new virus and malware threats emerge daily. Most of these programs will give you periodical reminders to “upgrade” to paid commercial or registered versions of the software, in some cases with some added features. The choice to upgrade is yours – but the important point is to use a product with anti-virus functionality, and which is up to date at all times.

Only install one anti-virus product on your computer at a time. Installing more than one product is not necessarily better and may create conflicts between the various products.

### **Don't be fooled into installing fake anti-virus software**

Fake anti-virus software has been circulating for a number of years and this type of malware relies on a number of methods to trick users into installation. By impersonating legitimate anti-virus packages, this type of malware will display fake warnings of computer infections and attempt to entice the user into installing or buying the product in order to clean their computer of viruses or malware. Some of these products are installed through web browsers and others from clicking links contained in spam e-mail. These products, which are really malware, can cause great disruptions for both home users and businesses, by either charging money for a service that they don't provide, and/or by harming the operation of the user's computers.

### **I have anti-virus software – do I also need anti-spyware software too?**

If using any of the products listed above, then, no. If using other products then it is important to read your product description to determine whether you need to install an AV and anti-spyware program, or whether you can install one product which provides both functions. As noted previously, many vendors now combine the anti-virus and anti-spyware functionality into a single product.



## Anti-spyware software

Spyware is a term commonly given to software that is installed secretly on a computer for the purposes of collecting information about a user, such as tracking their web browsing habits or other personal information. While some spyware is installed with the user's consent, the majority of spyware is often installed as a "drive-by download", usually the result of clicking on an option or link which is displayed in a deceptive manner and without the user's informed consent. The collected information is then relayed to advertisers or other interested parties.

Besides the collection of various types of personal information, spyware can also allow the installation of additional unwanted software on your computer and interfere with the correct operation of your web browser by redirecting you to pages that you did not request. This software can also be responsible for altering computer settings, which can result in altered browser home pages, slow connection speed, loss of Internet connectivity or the functionality of other programs.

As with anti-virus products, there are numerous anti-spyware products available, but some of the more popular products available to use freely for non-commercial use are:

Product	Link	Functionality <sup>4</sup>
Microsoft Windows Defender <sup>5</sup>	<a href="http://www.microsoft.com/windows/products/winfamily/defender/default.aspx">http://www.microsoft.com/windows/products/winfamily/defender/default.aspx</a>	Spyware only. This product is automatically disabled if Microsoft Security Essentials is installed.
Microsoft Security Essentials	<a href="http://www.microsoft.com/SecurityEssentials/">http://www.microsoft.com/SecurityEssentials/</a>	Combined anti-virus and anti-spyware

<sup>4</sup> If the product combines anti-virus and anti-spyware functionality, do not install another anti-virus or anti-spyware product on the computer at the same time.

<sup>5</sup> Windows Defender is automatically included with Microsoft Windows Vista and Windows 7. It is also available to download for Microsoft Windows XP Service Pack 2 or later from the Microsoft web site.



Lavasoft Ad-Aware Free	<a href="http://www.lavasoft.com/products/ad_aware_free.php">http://www.lavasoft.com/products/ad_aware_free.php</a>	Spyware and some types of malware covered by AV products but not all. <sup>6</sup>
Spybot Search & Destroy	<a href="http://www.safer-networking.org/en/index.html">http://www.safer-networking.org/en/index.html</a>	Spyware only. <sup>7</sup>

Only install an anti-spyware product if “spyware” protection is not included in the anti-virus product you are using. Installing more than one anti-virus or anti-spyware product may cause system conflicts and slow down your computer.

### **Don't be fooled into installing fake anti-spyware software**

Just as there are fake anti-virus programs, there are similar fake anti-spyware programs. These programs claim to be legitimate anti-spyware programs, but again are simply clones of the real software, attempting to encourage users to pay money for a service that they don't provide. They will generally tend to try to deceive the user through false warnings of infections and high pressure sales tactics. Often this software will offer free scans of infections but require payment to remove any spyware found. While most of these are deliberately fraudulent, others are simply sub-standard programs presenting false information. Sometimes these programs are actually themselves spyware.

### **Web-based online scanning**

Anti-virus online scanning programs work by connecting to a web site and requesting an “online scan” for viruses and other malware. Doing so may involve downloading a small piece of software, such as an ActiveX control.

While these online scanning web sites serve a very useful function they are not a substitute for having installed up to date anti-virus and anti-spyware software on your computer. Online virus scanners only have the potential to *detect malware that has already infected your computer*, whereas installed anti-virus and anti-spyware software have *the ability to prevent infections from occurring in the first place*.

<sup>6</sup> [http://www.lavasoft.com/download\\_and\\_buy/product\\_comparison\\_chart.php](http://www.lavasoft.com/download_and_buy/product_comparison_chart.php)

<sup>7</sup> <http://www.safer-networking.org/en/spybotsd/index.html>



However, anti-virus and anti-spyware products rarely detect 100% of all malware in circulation at any one time. Using an online virus scanner is an excellent way of checking whether the anti-virus and anti-spyware programs installed on your computer have failed to detect malware that has already compromised your computer.

Choose an online virus scanner with a brand that is different from the brand of anti-virus software already installed on your computer. It is not unusual for different anti-virus products to detect different malware. Running a free online virus scan weekly, or more often as required, provides an additional check to complement an existing anti-virus program installed. It is particularly useful to use when you suspect that you may have a malware infection on your computer which your existing anti-virus software has failed to detect.

There are many free online anti-virus scanning tools to choose from such as:

Vendor	Link	Comment
BitDefender	<a href="http://www.bitdefender.com/scan8/ie.html">http://www.bitdefender.com/scan8/ie.html</a>	Do not use if you already have BitDefender anti-virus software installed on your computer or network.
ESET	<a href="http://www.eset.com/onlinescan/">http://www.eset.com/onlinescan/</a>	Do not use ESET if you already have NOD32 anti-virus software installed on your computer or network.
F-Secure	<a href="http://support.f-secure.com/enu/home/ols.shtml">http://support.f-secure.com/enu/home/ols.shtml</a>	Do not use if you already have F-secure anti-virus software installed on your computer or network.



Microsoft	<a href="http://onecare.live.com/site/en-us/center/howsafe.htm">http://onecare.live.com/site/en-us/center/howsafe.htm</a>	The Protection Scan is available for Microsoft Windows operating systems only. Do not use if you have Microsoft OneCare or Microsoft Security Essentials software installed on your computer or network.
McAfee	<a href="http://us.mcafee.com/root/mfs/default.asp">http://us.mcafee.com/root/mfs/default.asp</a>	Do not use if you already have McAfee anti-virus software installed on your computer or network.
Trend-Micro	<a href="http://housecall.trendmicro.com/">http://housecall.trendmicro.com/</a>	Do not use if you already have Trend-Micro software installed on your computer or network.

Some of these products may recommend that you temporarily disable locally-installed anti-virus and/or anti-spyware products before conducting these online scans. If so, don't forget to re-activate these products after the online scan is completed. For more detailed information regarding online scanning programs, please see the Stay Smart Online [Factsheet 11, Part 2](#).

## Firewall software

A firewall is a system designed to block unauthorised access to or from a private computer network. Firewalls are frequently used to prevent unauthorised Internet



users from accessing private networks and computers connected to the Internet, and can also prevent many worms<sup>8</sup> and other types of intrusions.

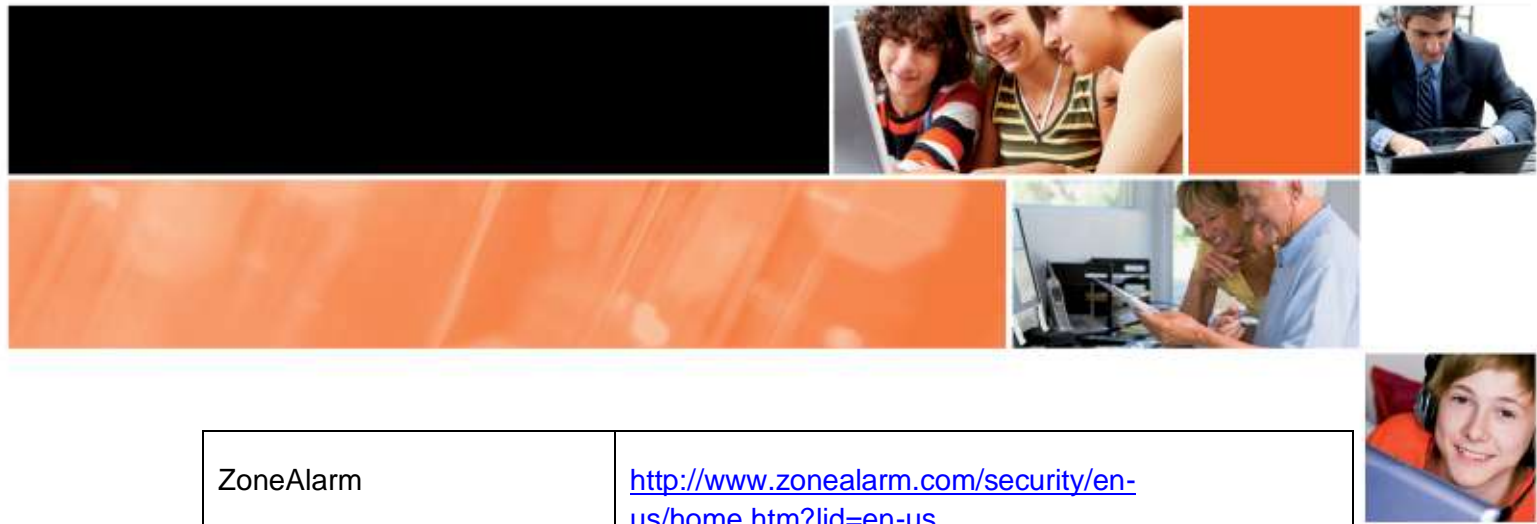
**How does firewall software work?**

A firewall monitors all of the traffic coming into and out of your computer. Any time that network access to your computer is requested, either from a program you are using (for e-mail, web browsing, downloading, etc.), or from other computers, a firewall will check its rules to decide whether to let the traffic in or out; or may ask the user to decide whether to allow or deny access. Firewall behaviour is based on a set of rules that are generated during its use, or can be manually created to allow or deny access for specific purposes.

Microsoft Windows XP (after Service Pack 2), Microsoft Windows Vista and Microsoft Windows 7 have a built-in firewall, known as Windows Firewall, however there are also a number of other free products which can be used instead of these. Information regarding Windows Firewall for XP, Vista and Windows 7, as well as links to some of the more popular packages available to use freely for non-commercial use can be found here:

Product	Link
Windows Firewall for Windows 7	<a href="http://windows.microsoft.com/en-us/windows7/Understanding-Windows-Firewall-settings">http://windows.microsoft.com/en-us/windows7/Understanding-Windows-Firewall-settings</a>
Windows Firewall for Windows XP	<a href="http://www.microsoft.com/windowsxp/using/networking/security/winfirewall.mspx">http://www.microsoft.com/windowsxp/using/networking/security/winfirewall.mspx</a>
Windows Firewall for Windows Vista	<a href="http://windowshelp.microsoft.com/Windows/en-US/Help/230d8c47-ee63-47e1-a1f6-a1d38b07dbee1033.mspx">http://windowshelp.microsoft.com/Windows/en-US/Help/230d8c47-ee63-47e1-a1f6-a1d38b07dbee1033.mspx</a>
Comodo Firewall	<a href="http://personalfirewall.comodo.com/">http://personalfirewall.comodo.com/</a>

<sup>8</sup> A worm is a form of malware that spreads by itself from one infected computer to another, including computers on a private network and across the Internet.



ZoneAlarm	<a href="http://www.zonealarm.com/security/en-us/home.htm?lid=en-us">http://www.zonealarm.com/security/en-us/home.htm?lid=en-us</a>
-----------	---

### Anti-spam software

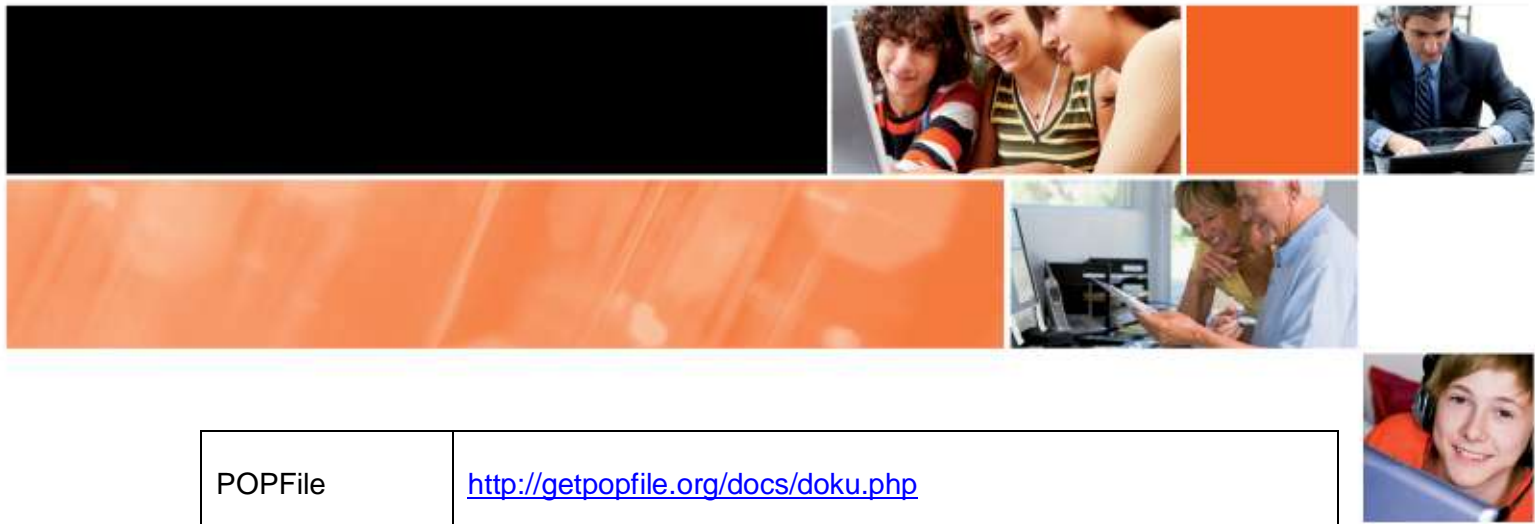
Most anti-spam software works by filtering the spam before it actually arrives in your e-mail inbox. Most internet service providers (ISPs) or e-mail providers (such as Hotmail or Google Mail) already conduct spam filtering of e-mail before it reaches your inbox, but these are not always completely successful, therefore it can be helpful to install anti-spam software on your personal computer.

Filtering can be done through a number of methods, such as via spam blacklists, scoring systems, or a set of rules created by users. Often these programs will integrate automatically with some of the more popular email clients such as Outlook, Outlook Express, Thunderbird and Windows Mail.

Additionally, to aid in the fight against spam, the Australian Communications and Media Authority (ACMA) has also produced a free tool – SpamMATTERS, which is designed for the purposes of reporting spam (not filtering spam). SpamMATTERS is free to download and install into the Microsoft Outlook and Outlook Express email programs. The tool will then allow you to both delete and report spam to ACMA simultaneously.

There are numerous packages available to filter spam e-mail which are available to use freely for non-commercial use, a number of the more popular packages as well as information regarding SpamMATTERS can be found here:

Package	Link
MailWasher	<a href="http://email.about.com/cs/winspamreviews/gr/mailwasher.htm">http://email.about.com/cs/winspamreviews/gr/mailwasher.htm</a>
BullGuard	<a href="http://www.bullguard.com/why/bullguard-spamfilter.aspx">http://www.bullguard.com/why/bullguard-spamfilter.aspx</a>



POPFile	<a href="http://getpopfile.org/docs/doku.php">http://getpopfile.org/docs/doku.php</a>
SpamMATTERS	<a href="http://www.acma.gov.au/WEB/STANDARD/pc=PC_310538">http://www.acma.gov.au/WEB/STANDARD/pc=PC_310538</a> <b>Note this product will not filter spam but allows you to easily report spam to ACMA.</b> It is not available for Windows 7 users.

## Are there risks installing these security software programs?

Yes. These security programs, like any other software, whether free or not, carry some potential risks. The programs themselves or browser software plug-ins may contain their own security bugs, which are later discovered and used by criminals to attack your computer. However, it is better to use these products than not – just be mindful of the need to check for new updates for these programs, once they are installed on your computer.

In the case of the AV and anti-spyware programs and online scanners, they only look for a specific set of malware and may not detect all malware with 100% reliability.

Similarly, firewalls can only block certain types of traffic; there are still harmful types of traffic which firewalls may still allow in.

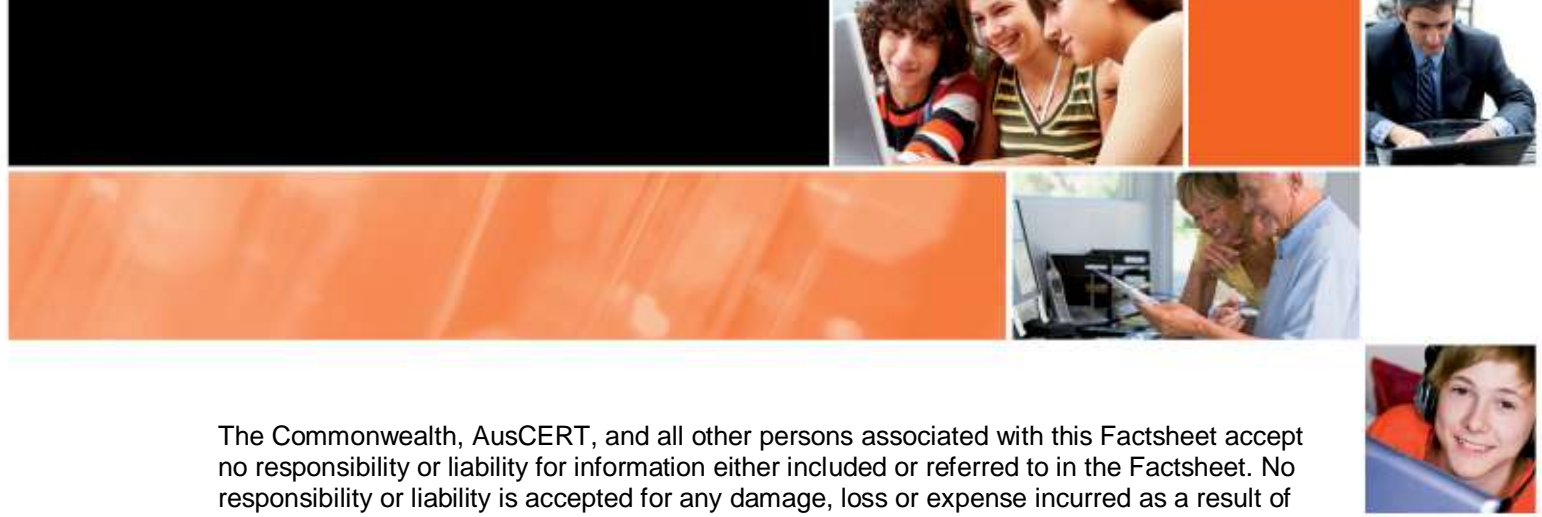
It is recommended you read the Frequently Asked Questions on the web sites for these programs before using them.

The programs mentioned in this factsheet are designed for home users and may not fully meet the needs of business networks.

### Disclaimer

This Factsheet has been prepared by AusCERT for the Department of Broadband, Communications and the Digital Economy. The information is intended for used by home users and small to medium sized businesses and is general information only and not intended as advice and was accurate and up to date at the time of publishing.

All software has the potential to contain bugs that may affect the security and/or stability of your computer. This software has not been evaluated by us and we provide no warranties for the software. Decisions to install and use the software are made at your own risk.



The Commonwealth, AusCERT, and all other persons associated with this Factsheet accept no responsibility or liability for information either included or referred to in the Factsheet. No responsibility or liability is accepted for any damage, loss or expense incurred as a result of the information contained in the Factsheet, whether by way of negligence or otherwise.

Updated June 2010

---

For more information go to [www.staysmartonline.gov.au](http://www.staysmartonline.gov.au)