



Australian Government

Department of Communications,
Information Technology and the Arts

TAKING CARE OF SPYWARE





Contents

Taking care of spyware	2
What is spyware?	3
How does spyware get onto my computer?	4
Removing spyware from your computer	6
How to prevent spyware from getting onto your computer	8
Other software that is not spyware	10
Who can help.....	12
More information.....	14



Taking care of spyware

Australians are using their computers and the Internet more and more to shop, bank, and do business. The Internet provides access to resources and services that would otherwise be time-consuming and difficult to reach in person.

While the Internet brings opportunity and convenience, it also carries e-security threats such as viruses, spam and spyware.

Taking care of spyware has been developed by the Department of Communications, Information Technology and the Arts (DCITA) to give you information about how to identify spyware, remove it and prevent it. It is supported by the Internet Industry Association (IIA) national anti-spyware campaign at www.nospyware.net.au, where you will find more detailed information.





What is spyware?



Spyware is software that is installed on a computing device and takes information from it without the consent or knowledge of the user and gives that information to a third party.

Spyware is an intelligence gathering tool—it is used to literally spy on people and collect information about them. People who install spyware may be targeting information such as banking and credit card details or other sensitive, commercial or private information. They may take this information for their own use or give it to another person. The presence of spyware on a computer can lead to serious consequences.

Although there is potential for spyware to be used on a range of computing devices, including personal digital assistants (PDAs)

and mobile phones, computers are presently the most common target.

Spyware can be used to collect personal information. It can collect email addresses for sending spam, or banking and credit card information that is then used to commit fraud.

Spyware that collects business information can be used to gain access to confidential or commercially sensitive records.



How does spyware get onto my computer?

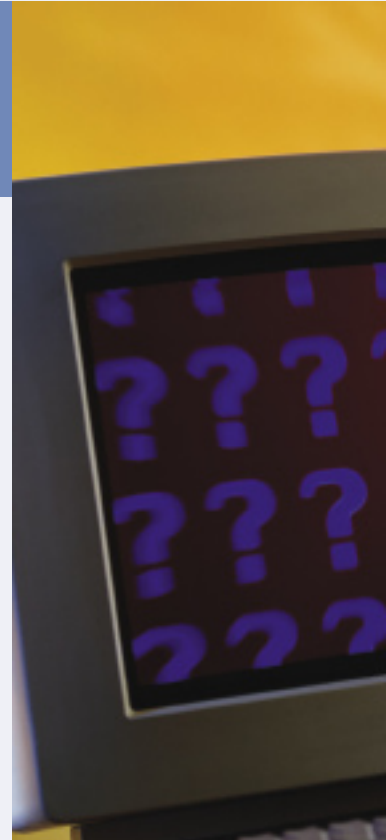
Misleading downloads

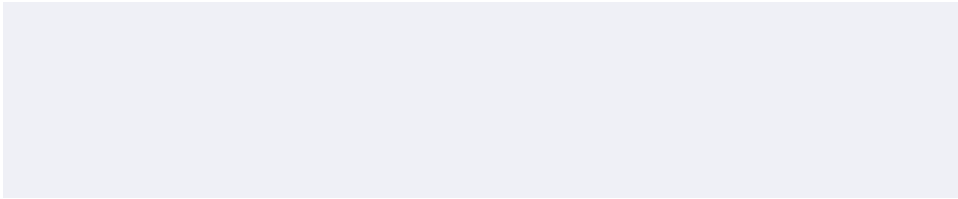
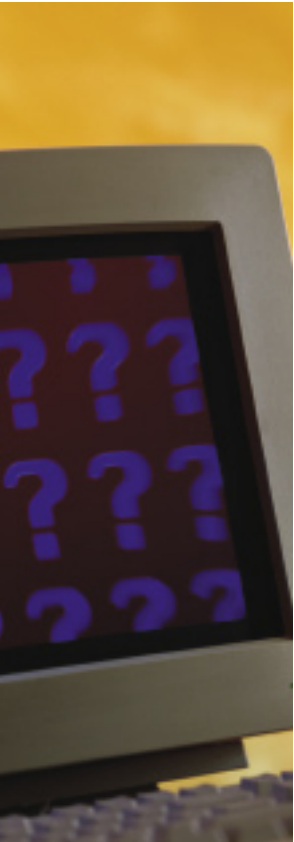
Spyware often uses trickery to encourage people to install it. These tactics range from fake alert messages to buttons that say 'cancel' when they really activate the installation. There are even cases of programs advertised as 'anti-spyware tools' that actually install spyware, rather than scanning for it and removing it.

Spyware may also be installed by a program that is attached to a webpage, pop-up window or email.

Bundled software

Some programs, particularly those available on the Internet for 'free', may place spyware on the computer when they are installed—the spyware is bundled with the desired program. Some of these programs mention the spyware in their terms and conditions, others keep it secret.





Security weaknesses

Like other malicious applications such as computer viruses, spyware can take advantage of security weaknesses on a computer. A computer without a firewall or anti-virus software is particularly at risk.

Symptoms of spyware

It can be difficult to tell if spyware is installed on your computer, because spyware is designed to run secretly in the background.

There are some signs that indicate that spyware may be on your computer:

- your computer behaves unusually and seems to have a mind of its own;
- random error messages appear;
- new toolbars or icons have been installed; or
- your antivirus and firewall software spontaneously turns off.



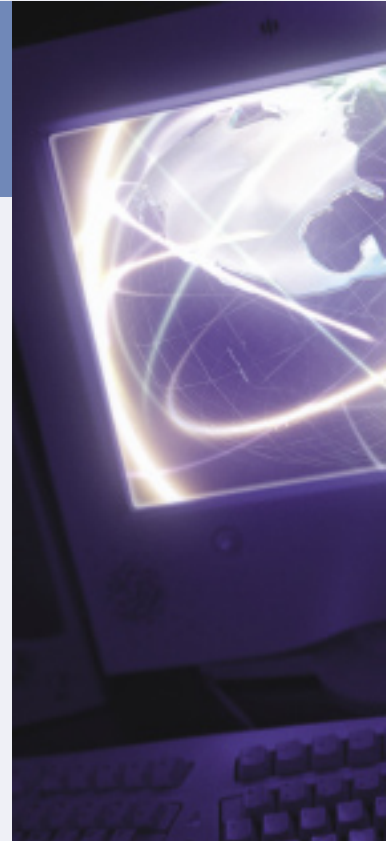
Removing spyware from your computer

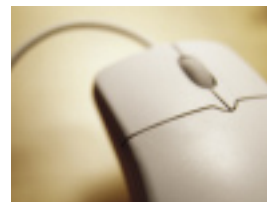
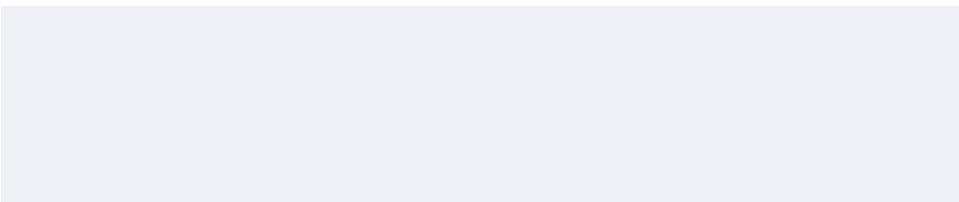
Spyware tactics that prevent removal

Most computer operating software includes functions that help manage the files stored on your computer. These functions commonly include the ability to remove or uninstall unwanted files and other programs from your computer.

Spyware, however, is increasingly being designed in ways that make it difficult to remove or uninstall.

One of the alarming trends is the ability of spyware to automatically reinstall itself. This is what makes it difficult to remove once it is installed on a computer.





Anti-spyware tools

The easiest and safest way to remove spyware from your computer is with tools that have been specifically designed to detect and remove spyware—or prevent it from being installed in the first place.

Anti-spyware tools are available as stand-alone products, and are also being built into anti-virus and other security products.

New forms of spyware are developed regularly as spyware creators find new ways of circumventing security tools. As a result, your security tools should be updated often.

Individual tools may be unable to remove all the spyware you may have on your computer. Some security tools detect versions of spyware that others do not. A combination of anti-spyware tools and anti-virus software may achieve the best results.



How to prevent spyware from getting onto your computer

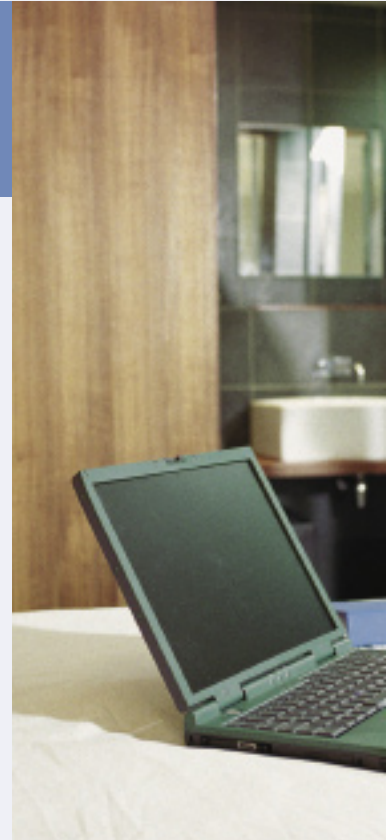
Security tips

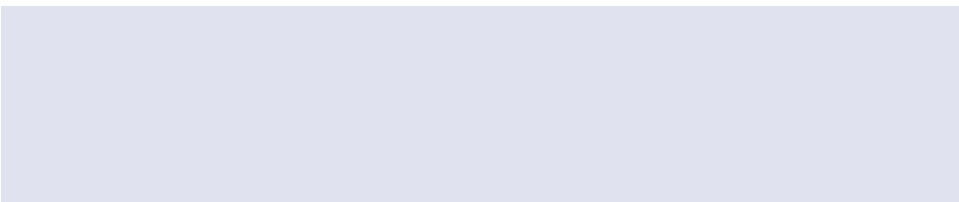
Develop good security practices. You need to have Internet security measures in place and have an understanding of how your computer works.

Install anti-spyware and anti-virus software and update it regularly. This will ensure that your computer is protected against the latest viruses and spyware.

Install a firewall. It will prevent unauthorised access to your computer and the installation of spyware on it. Some firewalls can also prevent information being taken from your computer and sent to someone else.

Be cautious with emails. Be cautious about opening emails from unknown or suspicious sources. Do not just look at the sender, also look at the body and the subject of the email. You should install spam filters to minimise the amount of spam you receive.





Back up your files. Create back-up copies of all your files and information to ensure easy recovery of information if needed. Always keep your backups in a different location to your computer.

Keep your software up to date. If your software is out of date you may be more vulnerable to spyware. Ensure that all your software is kept up to date. Watch out for the release of security updates and new versions of software.

Read terms and conditions carefully. When downloading or installing software on your computer, make sure you read the terms and conditions or any other licence agreements carefully. Be aware of what you are agreeing to.

Internet Security Essentials booklet

DCITA has published *Internet Security Essentials*, a booklet which gives greater detail about these security tips, and discusses other issues relating to operating safely online. You can find the booklet, designed for small business, at www.dcita.gov.au/e-security





Other software that is not spyware

Other software

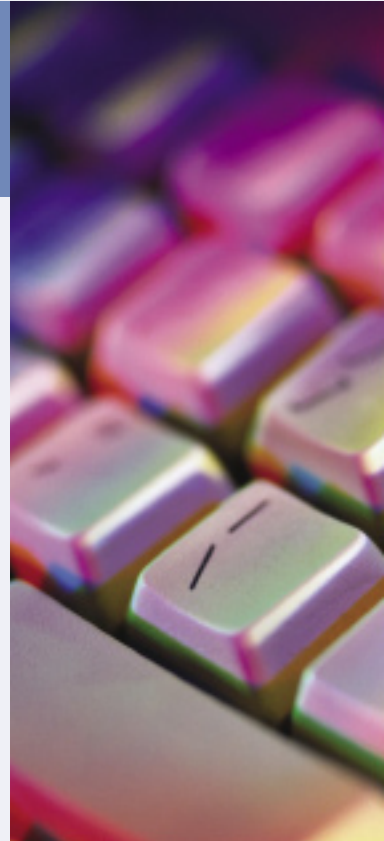
Legitimate software programs sometimes have elements that operate in a similar way to spyware. These include programs that have been designed to download security updates from the Internet, to prevent minors from accessing inappropriate material online, or to identify a user for subscription purposes.

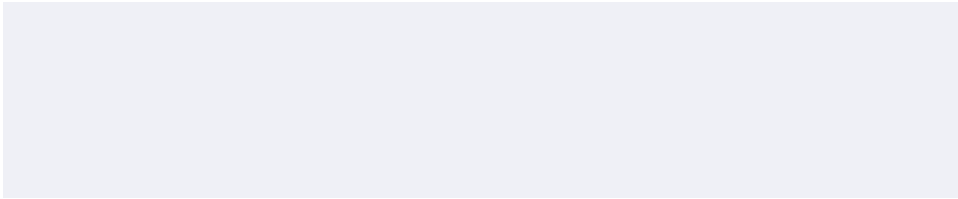
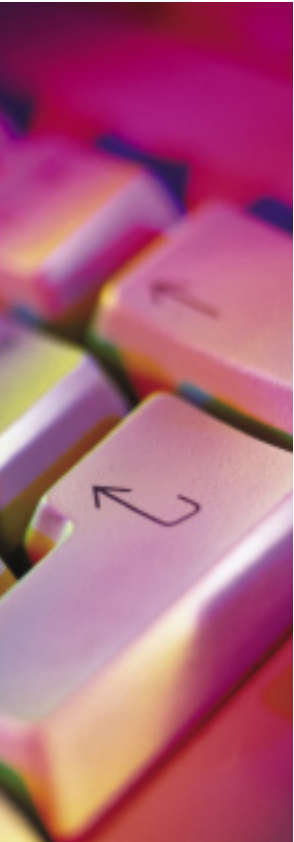
These programs send and receive information, however they are usually installed with your consent and agreement to the terms and conditions of use. You may choose to give permission for a program to be installed which will collect some personal information in return for something else, such as free software or games.

A more detailed discussion on legitimate software is available at www.nospyware.net.au

What is adware?

Adware is software installed on a computer to deliver advertisements or other content which encourages you to purchase goods or services. It is often installed through downloading free software. With your permission, some adware may also





collect information such as your web-surfing habits so that advertisements can be better targeted towards your interests. A more detailed discussion on adware is available at www.nospyware.net.au

What are pop-ups?

Pop-ups are also designed to deliver advertisements and other notices. Pop-ups are inbuilt features of particular websites and the ad is triggered when the website is visited.

What are cookies?

Cookies are small text and data files that a website places on your computer. Cookies can improve your surfing experience by recalling information such as the content

you have previously looked at and your colour and font size preferences.

Removal and uninstall options

There are a variety of methods available to help manage the different types of programs that may be on your computer. Most computer operating systems have 'add or remove program' functions which can be used to remove or delete unwanted programs.

Some software programs even have built-in uninstall functions.

There are also products designed to manage pop-ups and most Internet browsers offer functions to manage cookies.





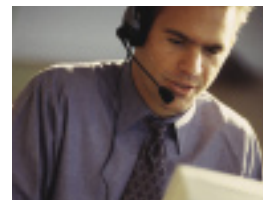
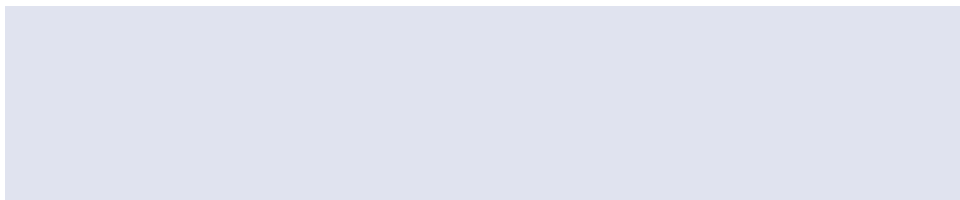
Who can help

Security and anti-spyware tools

The Internet Industry Association's national anti-spyware campaign at www.nospyware.net.au provides links to anti-spyware tools that are available free or for a trial period.

The Australian Consumers' Association's online CHOICE magazine provides the results of a test of nine free anti-spyware tools. This information can be found at www.choice.com.au. Click on 'spyware' from the A-Z index or type 'spyware' into the search function.





Where can I go to complain about spyware?

Complaints about high tech crimes such as online fraud and malicious software can be lodged with the Australian High Tech Crime Centre www.ahtcc.gov.au —click on the 'Reporting a high-tech crime' link.

You should also report online criminal activity to your local police.

The Office of the Privacy Commissioner deals with complaints about the handling of personal information by organisations. More information can be found at www.privacy.gov.au. Click on 'Individuals' and then 'Complaints'.



More information

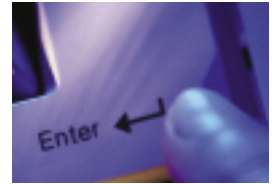
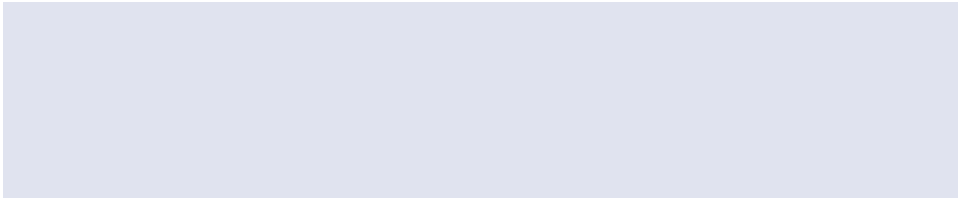
You can find more information about these topics on the spyware pages on the Internet Industry Association (IIA) national anti-spyware campaign at www.nospyware.net.au

General advice about e-security matters can be found at www.security.iaa.net.au

You can also find information about spyware on the DCITA spyware webpage www.dcita.gov.au/spyware

Information about e-security is available on the DCITA webpage www.dcita.gov.au/e-security





Taking care of spyware
is supported by the
Internet Industry
Association (IIA)
national anti-spyware
campaign at
www.nospyware.net.au, where you will
find more detailed information.



DISCLAIMER

The Department of Communications, Information Technology and the Arts (DCITA) has prepared this document to provide information. While every effort has been made to ensure that this document is accurate, no warranty, guarantee or undertaking is given regarding the accuracy, completeness or currency of the document. This information should not be relied upon as professional, commercial or technical advice. Links to other sources of information do not constitute endorsement of material at those sources or any associated organisation, product or service.

ISBN (hardcopy) 0 642 75304 0
(online) 0 642 75303 2

© Commonwealth of Australia 2005

This work is copyright. Apart from any use as permitted under the *Copyright Act 1968*, no part may be reproduced by any process without prior written permission from the Commonwealth available from the Department of Communications, Information Technology and the Arts.

Requests and inquiries concerning reproduction and rights should be addressed to the:

Commonwealth Copyright Administration
Attorney-General's Department
Robert Garran Offices
National Circuit
Barton ACT 2600

or posted at www.ag.gov.au/cca

DEPARTMENT OF COMMUNICATIONS, INFORMATION TECHNOLOGY AND THE ARTS
www.dcita.gov.au