



Spy-ware removal and awareness

Spy-ware is a computer related issue which is becoming increasingly apparent to business and home computer users alike. In order to help maintain a healthy and stable system and combat unwanted spy-ware it is necessary to perform regular maintenance. This maintenance may at first seem tedious and unnecessary, but this opinion usually only lasts until your first major attack of spy-ware.

There is a great number of anti-spyware solutions available on The Internet. Some of these programs are classified as 'free-ware' (available for free use), while others are share-ware (which means you may download, install and share the program for a set period before paying a subscription cost for further use. Such solutions include Lavasoft's Ad-Aware Personal, Webroot's SpySweeper, JavaSoft's SpyWareBlaster and SpyBot Search & Destroy.

Links to the download sites for all of the above programs can be found on our website – www.dcnetworks.com.au by clicking on the 'Downloads' tab on the menu bar and selecting the desired program. It should be noted that Ad-Aware, SpyBot and SpyWareBlaster are all free-ware applications and do not require a subscription – however, SpySweeper requires users to subscribe after the initial 30 day trial period.

You may ask why it is necessary to utilise so many applications – well, the reason is that despite thorough testing of many of the available solutions we have found that there is no 'one' application that we can safely say “removes *all* spy-ware”. Due to the complexity and vastness of spy-ware it is near impossible to have one application that will cater for all of your needs. With this in mind, Double Click advise the regular use of Ad-Aware and SpyWareBlaster. While Ad-Aware will remove many of the more common spy-ware elements, SpyWareBlaster acts as a shield which aids in the prevention of spy-ware before it infects you. In the event of heavy infection it may be necessary to adopt the use of SpySweeper and/or SpyBot.

While this combination of programs combine into a fairly comprehensive team, spy-ware developers are becoming increasingly cunning and are sometimes able to circumvent the counter-measures. In this case it may be necessary for a technician to perform manual removal of spy-ware from an infected computer.

Attached is an advised schedule for anti-spyware maintenance. This includes the steps required when confronted with varying levels of spy-ware severity:

- Phase 1 specifies procedures which should be carried out on a regular basis as a mean of general maintenance.
- Phase 2 specifies procedures which should be followed if you believe you are experiencing spy-ware related symptoms – eg) Internet pop-up windows, Spam E-mail, slow Internet browsing, slow general computing and some error messages.
- Computer service – At this point it is recommended to have the computer serviced by one of our technicians for manual spy-ware analysis and removal.

N.B. As each phase targets a more advanced degree of spy-ware infection the level of difficulty to utilise the removal tools increases. If at any point you feel that you don't understand the instructions, then a phone call is advised for further assistance.



Phase 1: - General Maintenance and mild spy-ware removal

This will include maintaining up to date definitions for both Ad-Aware and SpyWareBlaster, and running a general scan with Ad-Aware. For general maintenance it is advised to run an Ad-Aware scan on *at least* a weekly basis

SpyWareBlaster – download for free by following the link at www.dcnetworks.com.au

1. Double click the icon for SpyWareBlaster which should generally be found on the desktop.
2. Once SpyWareBlaster has loaded click on the 'Updates' tab on the bottom left of the window.
3. Next, after ensuring Internet connectivity, click on 'Check for updates' – this will connect to, check for and download any newer definitions required.
4. Once the download has completed click on the 'Protection' Tab at the top left of the window.
5. Now click 'Enable all protection.'
6. Now close SpyWareBlaster – this program does not need to be open in order to function.

Ad-Aware Personal – download for free by following the link at www.dcnetworks.com.au

1. Double Click the Ad-Aware SE icon which should generally be found on the desktop.
2. When Ad-Aware loads it may prompt you to check for the latest updates, if this is the case you should click 'Ok' and then 'connect'. This will search for any available downloads. If there are any newer definitions files to the one you currently have then Ad-Aware will ask you whether you would like it downloaded – click 'Download'.
3. If Ad-Aware does not prompt you to check for updates you should click on the 'Check for Updates' button on the bottom left of the Ad-Aware Screen and follow the remaining steps found in Step 2.
4. After clicking finish, you will now be presented with the main Ad-Aware menu. Click 'Start'
5. Ensure the circle is filled in beside “Perform Full System Scan”
6. Click 'Next' – this will perform a full spy-ware scan of your hard drive.
7. When the results are presented you should right click on any one of the items found and select 'select all objects'. This should place a tick in the box beside each spy-ware element found.
8. Click 'next'.
9. This will both Quarantine and remove the spy-ware elements that Ad-Aware has found on your system.

For users of Windows 2000, XP Home, XP Professional or 2003 Server, Microsoft have an Anti-spy-ware product of their own.

Microsoft Anti-Spyware – download for free by following the link at www.dcnetworks.com.au

1. Double click the MS Anti-spyware icon which should generally be found on your desktop.
2. Click on 'Spyware Definitions' which is towards the bottom on the left hand side.
3. Click on 'Run QuickScan Now' which is at the top right.
4. Click 'View Results'
5. Mark all objects found to be 'removed' by clicking on the drop-down menu next to each item.
6. Click 'Continue' and 'Yes' to finish the removal.
7. In some cases (on the first scan particularly) MS Anti-Spyware will present the ability to set default browser settings which may have been altered by spy-ware. If this is the case, click 'Configure Now'. The settings in the boxes are what is currently set, while the settings on the right are what are Microsoft Defaults. For most users simply clicking on each set of double blue arrows will re-define the defaults. Only in certain circumstances will users wish to alter the default settings, which can be done by manually entering the information in the respective box.

If you are still experiencing spy-ware related symptoms – such as pop-up screens, Internet Explorer being re-directed to illicit websites, error messages or slow computer performance you should proceed to phase 2.



Phase 2: - Moderate spy-ware infection

SpyBot Search & Destroy – download free version by following the link at www.dcnetworks.com.au

1. Double click the SpyBot icon which should generally be found on your desktop.
2. Click the 'Check for Updates' icon.
3. This will connect to, check for and download definitions from the server.
4. Select all items in the list which appear as being definitions or program updates. Skins and languages are not necessary.
5. Click download updates.
6. Click the 'Search and Destroy' icon
7. Click 'Check for problems'
8. Upon completion, ensure all items are checked and then click 'Fix selected problems' and then 'yes'.
9. Click 'ok'

SpySweeper – download trial version by following the link at www.dcnetworks.com.au

1. Double click the SpySweeper icon which should generally be found on your desktop.
2. On the list of options on the left hand side click 'Options'
3. Next click 'Update Definitions' – this will enable SpySweeper to connect to, check for and download any new definitions.
4. Next click on the 'Sweep Now' option at the top left of the window.
5. Click 'Start' – this will perform a scan of your computer for any spy-ware related material
6. Upon completion click next.
7. Next click 'Select all traces' and click 'Next' and 'Finish'
8. Click the close cross at the top right hand corner of the window and select 'shut down'.

If you are still experiencing difficulties with web browsing or other spy-ware related issues a computer service is recommended where a Double Click technician can perform spy-ware analysis and removal and any further repair that may be required.

Double Click technicians can either work on your computer in your home or office or you may elect to have the computer serviced in our shop. Please note that while On-site repairs are sometimes more convenient, the labour cost for a shop repair is always capped at 2 hours.

In order to make the time spent by the technician as time (and cost) effective as possible, it is advised that you present a log of problems you are receiving. An exemplary log would appear as follows:

<u>Problem:</u>	<u>Time - Date:</u>	<u>Description:</u>
Internet Pop-up	7:30 – 21/4	Was reading the news on www.smh.com.au and received a pop-up informing me I had spy-ware.
Web-page redirection	8:00 – 21/4	Attempted to visit www.google.com however was presented with an illicit website and popups.

*THIS BULLETIN IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. The information contained in this document represents the current view of Double Click Networks Pty Ltd. on the issues discussed as of the date of publication. Because of the wide variety of individual PC configurations, both hardware and software, information provided in this document is provided "as is", without warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose and freedom from infringement. The user assumes the entire risk as to the accuracy and the use of this document.