



ANTI-SPYWARE SECURITY

WHAT IS SPYWARE?

“Spyware” is a term used to describe computer software that exhibits certain unwelcome behaviours, such as changing your notebook configurations, tracking personal information, or bombarding you with pop-up advertisements. The key to spyware is that it is installed on your notebook without your explicit consent or knowledge.

HOW DOES SPYWARE GET ONTO MY NOTEBOOK?

Spyware is most typically an unwanted byproduct of installing software that you actually do desire. The fact that you will be installing additional software is usually buried somewhere in the End User License Agreement. Although you must agree to the terms of the License Agreement before proceeding with any Internet download, distributors of spyware are banking on the fact that many people just skim over these agreements, if they even read them at all. For this reason, it is important to carefully review all license agreements and privacy statements before downloading software from the Internet.

Enterprising hackers can also remotely install spyware programs on to your notebook, if it isn't adequately protected. Depending on the stringency of your browser security settings, spyware can also be installed on your computer as you pass through certain web sites.

HOW CAN I TELL IF SPYWARE IS ON MY NOTEBOOK?

Typical signs that spyware has been installed on your system include:

- Your notebook is running much slower than normal
- Your web browser home page keeps changing of its own accord (and can't be reset back to your original home page) or you are unable to browse to a desired site because spyware is redirecting your browser to preset pages
- Pop-up advertisements appear on your screen, even when you aren't browsing the Internet
- Your web browser crashes or closes, suddenly and repeatedly
- There is a new toolbar in your web browser that you didn't put there

WHAT SHOULD I DO IF SPYWARE IS ON MY NOTEBOOK?

There is a good reason why spyware is difficult to remove from your notebook: it was designed that way! Thankfully, there are products available that can purge your system of unwanted spyware.

NORTON INTERNET SECURITY — ANTISPYWARE EDITION

This program is designed to detect and remove spyware and other non-viral security risks. For information on how to use this product, please visit:
<http://service1.symantec.com/SUPPORT/nip.nsf/docid/2005022315283436>

OTHER ANTI-SPYWARE PRODUCTS

There are a number of anti-spyware applications available for download from the



Internet, including **Microsoft Windows Defender, Sunbelt CounterSpy, Ad-Aware** and **Spybot Search & Destroy**.

For those that are “freeware” applications, which means they can be downloaded at no cost to you, there is no associated technical support or warranty as to their effectiveness.

NOTE:

Toshiba does not endorse any specific freeware or share utilities designed to remove spyware applications. The use of spyware removal software may conflict with end user agreements of other applications installed on your system. Please consult your user license agreements for further information.

5. HOW CAN I PREVENT MY NOTEBOOK FROM GETTING INFECTED WITH SPYWARE?

There are several steps you can take to prevent your notebook from getting infected with spyware:

- **Adjust your browser settings** – Your browser security setting should be set to medium, or higher, to prevent spyware from being installed on your notebook while you navigate the Internet
- **Browse safely** – The best policy for avoiding spyware would be to never download free software from the Internet. However, since most people do, the next best advice is to only download content from trusted or reputable sites. Before you download, always read user agreements and privacy policies in their entirety to avoid receiving extra software that you weren’t expecting, and don’t want.
- Don’t forget to be judicious when dealing with email attachments as well: they are another vehicle for spreading spyware. To avoid infection, only open email from sources you recognize and trust.
- **Use a firewall** – A firewall will provide solid defence against hackers trying to place spyware on your computer. If your firewall also offers outbound protection, it will block installed spyware from sending out communications regarding your system without your knowledge.
- **Install anti-spyware software** – There are many good anti-spyware products available on the market. Anti-spyware software protect the system by preventing spyware from being installed on it. See the section in this document entitled “**What should I do if spyware is on my notebook?**” for more information on anti-spyware software.
- **Keep your software updated** – Keeping your operating system updated with the latest critical security updates also helps to protect your notebook from spyware. Microsoft Update can help you manage this process at <http://update.microsoft.com/microsoftupdate/v6/default.aspx?ln=en-us>.

CAN I USE BOTH ANTI-SPYWARE AND ANTI-VIRUS SOFTWARE?

You can, and you should! Anti-spyware software only detects and removes non-viral security threats. As such, it doesn’t protect your notebook from viruses, worms or Trojan horses. For protection against these types of malicious software, you also require anti-virus software (see our FAQ on this subject for more details). Most anti-virus software is compatible with anti-spyware software, enabling both



to be installed at the same time. Many anti-virus products now include built-in anti-spyware functionality, eliminating the need to install two separate programs.

HELPFUL LINKS

Symantec™ Antispyware
<http://enterprisesecurity.symantec.com>

Ad-Aware®
<http://www.lavasoftusa.com>

SpyBot Search & Destroy
<http://www.spybot.info>

Microsoft Security at Home
<http://www.microsoft.com/athome/security/default.mspix>

Microsoft Windows Defender
<http://www.microsoft.com/athome/security/spyware/software/default.mspix>