

Spyware & Malware

July 2007

Look out! There's a SPY about!

Our E-Business Advisers take you on a journey into the murkier bits of the Internet.....all the better to protect yourself:

1. What are "Spyware" & "Malware"?

The terms "Spyware" and "Malware" relate to software which is unknowingly installed on your PC by you.

Spyware covertly gathers information about you and your PC through your Internet connection.

Malware is just the generic name for all sorts of software nasties that you really don't want on your PC - that includes Spyware!

They are mini software programs, and are typically hidden components of freeware or shareware programs that you've downloaded from the Internet.

2. What does Spyware & Malware do?

Once installed, spyware monitors your activity on the Internet and transmits that information in the background to someone else.

Spyware can also gather information such as email addresses, passwords and even credit card numbers.

Spyware programs differ from computer viruses in that they do not usually self-replicate.

Spyware is almost always designed explicitly for commercial or financially fraudulent exploitation of the host computer.

This shows itself in different ways:

- Monitoring and reporting back to the originators of your browsing habits for commercial purposes.
- Gaining access to your passwords and credit card numbers, and sending them back to an offender.
- Sometimes, the delivery of unsolicited pop-up advertisements with no control on your part.
- Re-routing of your web browser to web sites, which are filled with advertisements profitable to the offender.
- Other types of Malware likewise have negative effects:
 - If you are still on a dialup Internet connection, this adjusts your PC's dialup settings to connect to the web premium rate telephone numbers, (without your agreement), earning income for the offender.
 - Called "Premium rate diallers" or "rogue diallers", this malware causes large volumes of complaints to telecom providers each year, when the subscriber receives an enormous telephone bill.

Fact Sheet

- Their dialup connection has been hijacked, and they could be paying £1.50 a minute for their Internet connection!
- Changes your web browser “Home” page, and creates new bookmarks in your Favourites folder, in the hope that you’ll visit these sites.
- Often, changing the web browser home page back to what it should be doesn’t work - the malware constantly re-sets it back again.
- Displays strange icons and or shortcuts to new software on the desktop - with no obvious uninstall route either.

3. How do I avoid Spyware /Malware?

To help avoid Spyware / Malware threats, it’s wise not to download or install software from any ‘unknown’ resource that you may come across on the Internet.

If the offer is bogus, this could become a costly, disruptive mistake.

Although there are many useful Freeware and Shareware programs on the Internet, you do have to exercise caution, as sometimes the reason the software is free is that it’s got a hidden “surprise” built in!

This is not that common, but does occur. (See “Freeware and Shareware” Fact Sheet in this series for more details).

Likewise, be very careful about getting “click happy” - by which we mean if a windows pops up whilst you’re browsing the web, saying “Do you want to install XXX software....” - your answer should be NO.

This is a common method for installing on your PC the rogue diallers discussed earlier, as well as a lot of spyware too.

It is also not a good idea to download any Toolbar programs for Internet Explorer - with the exception of the Google toolbar and the Yahoo! toolbar - both are safe.

Luckily, there are plenty of free software applications enabling detection and removal of spyware / malware by scanning your PC, memory, drives and devices for aggressive marketing, rogue dialers, tracking components and other spyware /malware.

There is no "one size fits all" solution to the problem of spyware / malware – but the growing trend of downloading resources from the Internet opens up the potential for security risks, unwanted and unsolicited access to you and your computer systems.

4. What to do....

- Always make sure you have updated your Microsoft system to get at least all the critical updates they release. To do this, in Microsoft Internet Explorer, go to “Tools” on the top menu bar, then “Windows Update”, and follow the on-screen instructions.
- Install and use anti-spyware / malware programs - links below

5. Useful Links

www.io.com/~cwagner/spyware -

A “must read”, very informative site, covering in good and understandable detail the threats faced.



Fact Sheet

www.spybot.info -
Free, good downloadable anti-spyware /
malware program.

www.lavasoft.de -
Free, good downloadable anti-spyware /
malware program.

Use both the above together - anything missed
by one should be picked up by the other.

Your anti-virus software suite may also have
some protection built in, or an "add-on" element
you can purchase to address this threat too.

*Disclaimer: we have no commercial links with
these companies or their products, and their
appearance in this fact sheet is not an
endorsement.*