

# Dealing with Viruses and Spyware

Most businesses, particularly those that have a permanent connection to the Internet, will have at some stage experienced either a virus attack, spyware or both. There is much confusion on how these threats spread, and perhaps more importantly, the “best practice” on how to deal with these threats.

## Viruses

### What is a computer virus?

A computer virus is a program with the characteristic feature of being able to generate copies of itself, and thereby spread. The mischief caused can be very minor, such as causing a funny image or cryptic message to be displayed on your screen, or it can do some serious damage by altering or even destroying files. For example: the Chernobyl virus overwrites the beginning of the hard disk on certain dates.

### Defending against viruses.

For a computer virus to “infect” a computer, the virus program needs the ability or “permission” to make changes to the target computer. In simple terms, the virus program will attempt to modify files and/or registry entries on the “target” computer. Once these changes have been made, the destructive payload will then be activated under certain conditions (e.g. when a certain date/time occurs, or when the user performs a certain act (e.g. starts a particular application etc)).

### Standard Operating Environment (SOE)

Therefore an effective approach to blocking viruses, which in our experience is often overlooked, is to configure the target computer in such a way that by default programs do not have “permission” to make changes to the underlying operating system. This is done by implementing a “Standard Operating Environment” (SOE). You can learn more about a SOE [here](#).

One of the features of a SOE is ‘lockdown’. The term 'lockdown' refers to using security features and policies available in the operating system to restrict the user's ability to re-configure their PC. This is required to ensure that PC's implemented in a 'standard' manner remain standard. One of the by products of ‘lockdown’ is that virus programs – like users - are restricted in the changes that they are able to make to the target computer.

## Anti-virus Software

The most common method employed to defend against computer viruses.

The primary method an Anti-virus product uses to detect viruses is by scanning files using a virus database. Most products will have a scanner that scans files either in memory or accessed as well as a scheduled scanner that performs scans at a predefined time.

The virus “definitions” are similar to a dictionary that includes a “signature” for each virus identified. The signature is a unique piece of code used to identify the virus.

A common misconception is that if you have an anti-virus software product installed, then you’re automatically protected against all viruses. In a perfect world this might be true, but we don’t live in a perfect world. Two reasons why anti-virus software is not always effective:

1. The virus definitions installed on the target computer are not current.

Occasionally this can occur because the update mechanism “breaks”. Like backups, anti-virus software needs to be regularly monitored to ensure that the definitions are current on all systems (with a good product this check can be performed from a central console).

Alternatively we have seen instances where a site has inadvertently allowed their virus definition subscription to lapse; again this would become apparent with regular monitoring.

2. There isn’t a virus definition for the virus as yet.

This is a rare scenario, but one that we have observed. It is possible for any anti-virus product to miss a virus, as the definitions themselves are generated from reports of virus “infections”. That is, someone has to first be infected by the virus, before the anti-virus vendor becomes aware that a new virus exists – and then they write a new virus definition.

Thus “best practice” to defend against computer viruses is to implement a multi-pronged approach:

1. Implement a SOE.
2. Deploy one anti-virus product on your desktops and servers.
3. Deploy a second anti-virus product specifically for e-mail (a frequent source of viruses), which means that you have two independent virus definitions scanning e-mail.

## Spyware

### What is Spyware?

Spyware is a computer program that, when installed on your computer, changes settings, displays advertising, and/or tracks Internet behaviour and reports information back to a central database. Spyware is often installed unintentionally by users along with other wanted software, and can be very difficult to remove. Spyware is also known as malware or nastyware.

Although some may argue that the distinction between Spyware and Viruses is starting to become blurred, the characteristics that make Spyware unique from a virus are:

1. Spyware programs are generally not destructive themselves, in that they don't delete data or files. Although if Spyware programs are able to capture user passwords and communicate these to a third-party, then there is the potential for destructive consequences indirectly.
2. Spyware is however often very disruptive, in that the programs often change the display settings of the PC, and frequently install "pop-up" advertising or "browser hijacking" modifications.
3. Spyware attacks – to date – have been implemented primarily via exploits in Microsoft's Internet Explorer web browser. Other web browsers (e.g. Mozilla, Firefox, and Opera) do not appear to be as vulnerable, although of course this may change in time.
4. Spyware is often not detected by many Anti-virus software products.

Spyware has started becoming a real issue over the last 6 months as the volume and technical sophistication of the exploits has advanced (which is not to say that we're impressed by spyware authors – we're not). Once Spyware is installed it can sometimes be incredibly difficult to remove; in certain instances it can be more economic to "cut your losses" and perform a full re-install.

Most computers are infected by browsing a web site with Internet Explorer. Whilst so called "unsavoury" sites are well known for causing issues, there are unfortunately many sites that can infect a computer. As Internet Explorer has many security loopholes it can sometimes be exploited by the web site to install the payload without warning the user. More often though, the user is 'tricked' into accepting a warning dialog box through clever 'social engineering' techniques.

Firewalls are generally unable to block this type of activity as it is technically requested by the user (even though they may not be aware of it).



## **Defending against Spyware.**

### **Education**

Users may attempt to install un-authorised software unwittingly due to a lack of understanding of the potential consequences. The lure of "free" software that purports to provide some 'nice' feature like an automatic desktop-changer, or an exotic screen-saver is designed to encourage users to download and install a program. What users often don't appreciate is that these programs from an unknown source may also contain Trojans (e.g. a second 'hidden' program) such as the pop-up advertisements or worse remote keystroke monitoring software to capture passwords and other confidential information, or some other 'nasty' like a virus).

Unauthorised software can also be installed automatically without the users' knowledge when visiting certain undesirable Web sites. Often these "honeypot" sites lure users with the promise of free give-aways, or other dubious material. Once the user visits the Web site, the Web site exploits vulnerabilities in the web browser to automatically install and execute Trojan software.

The first and cheapest step is educating users about "acceptable use" policy of computers in the work environment. If users don't install un-authorised software, and users don't visit non-mainstream Web sites, then the risks of installing Trojan software is substantially reduced.

### **Standard Operating Environment (SOE)**

As with defending against computer viruses (refer above), employing the 'lockdown' feature of a SOE is an effective strategy in blocking Spyware.

### **Change your default Web browser**

Because the vast majority of Spyware "installations" are at present executed via Microsoft Internet Explorer (IE) vulnerabilities, avoid using IE except where absolutely necessary by changing the computer's default web browser. Mozilla Firefox, to date, has proven to be far more secure than IE and has built-in security to block most Spyware resident on a web site from installing on the target computer without at least warning the user first.



## Anti-spyware software

Some corporate anti-virus products are now starting to defend against Spyware, although at this stage our view is that some anti-virus vendors appear to be playing 'catch up' in this area. Nevertheless by choosing an appropriate anti-virus package for your desktop, you can strengthen your defences against Spyware.

There is also a range of dedicated anti-spyware programs that are available, some freeware (e.g. [Ad-aware](#), [Spybot Search & Destroy](#)) and some commercial. However from our experience to date, if you follow the tips we have provided here, commercial Spyware packages should not be required to prevent "infection". On the other hand, some of the commercial packages can be an economical option in "cleaning" a heavily infected computer.

---

---

---

---

---

---

---

---

Zero Effort Networking (ZEN) is experienced in accurately identifying computer network problems and acting swiftly to fix them. Since 1996 we have helped clients implement stable, reliable computer networks that take the worry out of network management. For further information you are welcome to contact us.

Zero Effort Networking Pty Ltd  
ABN: 38 082 434 446  
Telephone: 02 9676 3541  
Facsimile: 02 8569 2012  
E-mail: [info@zeroeffortnetworking.com.au](mailto:info@zeroeffortnetworking.com.au)  
Web: [www.zeroeffortnetworking.com.au](http://www.zeroeffortnetworking.com.au)  
Office: Suite 15, 18 Third Avenue, Blacktown NSW 2148

No part of this publication may be reproduced without written permission of the authors. Copying and distribution by any means is strictly forbidden. Additional copies may be obtained for free by contacting Zero Effort Networking.