

## **Information Is Power – Dealing With Internet Security Concerns by Staying on Top of the Latest Developments**

*New forms of malicious software are created every day and even with a high quality Anti-Virus program installed it is important for the Internet user to stay updated regarding the latest threats and detected vulnerabilities*

Supportcave is therefore now offering a new TechBlog for everyone who wishes to keep a jour with the latest developments in computer security. The TechBlog at Supportcave.com is focused on seven different areas regarding Internet security – Spyware, Spam, Anti Virus, Trojan Horses, Firewalls, Internet Security and Computer Privacy.

Since new forms of wicked software such as Spyware, Adware and Hijacking programs are constantly being created by corrupt programmers, the Internet users of today can not just install an Anti Virus program and then lean back, thinking that they will be 100 percent protected from any attack from malicious software. The present forms of malicious software utilize a wide range of different methods in order to stay undetected by the Anti Virus programs. Every Internet user should keep a jour with the latest trends and developments in order to find out the most up-to-date way of protecting his or her computer from attacks.

The oldest forms of concealed computer viruses simply used a method where they made sure that the “last modified” date of the infected file remained unchanged, even though a major change had in fact taken place when the file became infected with the virus. With the development of the Anti Virus programs, this method became obsolete and the shady programmers had to find new ways of concealing their creations.

With the invention of the so called Cavity Virus, detecting infected files became increasingly difficult since the cavity virus can infect a file without damaging the file or even increasing the file size. This is possible since the cavity virus will overwrite unused areas in executable files. A well known example is the so called Chernobyl Virus (CIH) that infects portable executable files. The Chernobyl Virus has a size of 1 KB, but the infected file will not grow one 1 KB larger.

The next step by the virus creators was to invent viruses that could actually attack the Anti Virus programs. It is also common for viruses to be programmed to stay away from files belonging to Anti Virus programs, since Anti Virus programs will integrity check their own code and rapidly detect any infected files. By staying away from the Anti Virus program, the Virus is less likely to become detected. Modern viruses will also avoid so called “bait files” or “goat files” that has been deliberately created by the Anti Virus company in order to attract viruses. Each time an operating system is changed, the virus programmers will find out new techniques for their software and benefit from any security vulnerabilities associated with the new operating system.

As you can see, it is important to rapidly find out about new security problems since old Anti Virus programs can be incapable of detecting new viruses. If you want to find out about new security treats before your computer becomes infected with a virus that your old Anti Virus program is incapable of detecting, check in regularly at <http://blog.supportcave.com/>.

### **Contact Information**

For more information contact Jason Frovich of Powertec Computers (<http://www.supportcave.com>)  
204-261-4406

**Keywords**

[malicious software](#)

[Anti Virus program](#)

[wicked software](#)

You can read this press release online [here](#)