# CNS eZine: Virus Protection is Serious Business May 2003

Last month's article discussed several ways to secure and tune-up your computer. This month's article will discuss virus protection, in depth.

**Fact**: There are more than 80.000 known viruses that have been found by May 2003.
**Fact**: Viruses are written by pretty clever programmers, mostly with the intent to destroy data, use your pc to help distribute the virus, and possibly steal information (credit card numbers, social security numbers, bank account numbers, Social Security numbers, and as much personal data as possible).

Lets take a closer look at each type of virus:

**Destroyers** attack the files on your computer, often deleting or overwriting your operating system's files with their own. It's difficult to tell when this happens, since most viruses are meant to run undetected by the user. Only a few viruses have one sole purpose, to render your hard drive useless.

**Identity Theft** can occur on non-secure online transactions, most of us already know that. Stay with the names you know on the net for your purchases, you're typically safe with the big names. However, if your pc has been compromised with a virus that its sole intent is to gather personal information and report back, you could be unknowingly feeding information to a criminal. Our best suggestion is to reserve one credit card for online purchases, and use it for just that. In case of theft, you only have one call to make, and you won't disrupt the other card-carrying persons by canceling their cards as well.

**Firewalls**: Enterprise users with dedicated internet connections have to take an important extra step. If your company has an IP address, or has a server that hosts your company's website, you need a good firewall. A firewall is a software application that provides security against hackers breaking into your network. Once they're in, they're typically in the identity theft mode, so make sure your network has security facing the outside world. Guess what? That includes those who use cable modems, and DSL connections as well! I had a neighbor with cable internet access and noticed the hard drive busy while nothing was running. A quick check found that a hacker had gained access and was using his pc to spread bogus email spam, and remain anonymous.

**Where do they come from?** Most anywhere or from anyone! You could get an attachment from a friend or relative whom you trust, but its not the person you need to trust, it's the integrity of their pc you need to be trusting. Basically-speaking, if you don't know the person, or didn't request an attachment, or do know the person but don't trust their pc security skills, don't open the attachment, unless of course your pc is protected with current virus protection software.

All software manufacturers have their own way of monitoring your system, but each consists of their main control program, and a "signature" file. The signature file is an example of every known virus found to date, so its important to configure the program to

“automatically update”, which means the software will look for a signature file update when you’re online, and if it finds one, it will download it and begin using it, all without the hassle of you having to remember to do it yourself.

Good resources for virus protection software can found at http://www.symantec.com , http://www.mcafee.com , and http://www.grisoft.com , and several others. Of course, if you want a professional to analyze your PCs and network and cure virus issues if they exist, just let us know.

Sincerely,

Your friends at Competitive Network Solutions, Inc.
Memphis, TN
901-757-0379
sales@CompetitiveNetworkSolutions.com
www.CompetitiveNetworkSolutions.com