



*The following article appeared in the June 19, 2009 issue of New Hampshire Business Review.*

## **Guarding against computer viruses**

By Marc Berthiaume

It has been about 26 years since the creation of the first computer virus. Today, the number of viruses has increased to over 250,000, and each one has the potential to damage your computer and your business — damage that ranges from bothersome to devastating — and can be very costly.

Companies are hit on average with 113 virus infections every month for every 1,000 PCs they own, according to an ICSA Labs survey.

According to a 2006 FBI report on computer viruses, “dealing with viruses, spyware, PC theft and other computer-related crimes costs U.S. businesses a staggering \$67.2 billion a year.” Every business, large or small, needs to protect against computer viruses. If you download files from the Internet or share files with outsiders, you stand a chance of getting a computer virus.

How does a business guard against this threat? First, it’s helpful to understand what a computer virus is. A good definition is offered by Amer Neely in “Virus Protection Rx for Your PC”: A virus is a program that attaches itself to other programs and/or disks and makes copies of itself whenever it can. It is vandalism by computer. Most viruses cause damage, either by design or accident; others merely become a nuisance by putting messages on your screen.

The important thing to remember is that someone wrote the program on purpose. Viruses do not appear out of thin air or by accident. In all cases, you will have to scan your hard disk and all your external disks and remove the culprit.

Viruses attach themselves to other files that are “executable.” This means any file that can be loaded into your computer’s memory and “run.” Files ending in .exe, .com, .sys, .dll and .ovr are some common PC extensions for executable files. Image files (.jpg; .gif) are not good hosts for a virus, since they are not executable. Audio files and video files are other “safe” types. A compressed file, such as .zip, by itself is not dangerous, but it may contain an executable file, which carries a virus. If this file is extracted and run, the virus will infect your system.

### **Basic virus protection**

Some common symptoms that could indicate your system is “infected” by a virus are:

- Unusual messages or displays on your monitor
  
- Unusual sounds or music played at random times
  
- A changed file name
  
- Missing programs or files
  
- The creation of unknown programs or files
  
- Files that become corrupted or suddenly stop working properly
  
- E-mails sent out to people on your mailing list or contact list without your knowledge



Don't wait until you have these symptoms to take action. The consequences could be alarming. Here are some basic tips that you can use immediately to start the fight against harmful computer viruses:

- Keep up to date with critical software patches. The most damaging viruses in recent years have all been spread through software vulnerabilities that were patched at least months, and often years, before the virus was unleashed.
- Don't open attachments that you did not expect to receive, especially if the person has not signed his or her name inside the message — and do not forward them.
- Delete all messages from unknown origins without reading them.
- Buy a virus protection program and keep it up to date. New viruses are detected and created daily and you must continue to update this software. Download the anti-virus update on a weekly basis.
- Use the latest versions of Web browsers. Virus writers are ingenious in a twisted way. They are always coming up with new attacks, oftentimes exploiting weaknesses in commonly used software. Software developers play a cat-and-mouse game, constantly trying to patch the holes with software upgrades and service releases.
- Set your security settings on “medium” or “high” for your e-mail reader and browser.
- Make sure you enforce a rigid backup schedule. If all of the above methods fail you and your data is gone, you must have a backup to save the day.

Keep in mind that these suggestions are just the tip of the iceberg when it comes to protecting your business from the serious threat of computer viruses. Virus protection should be an integral part of IT planning. Since it can be very complex, it should be handled by knowledgeable, highly trained IT professionals.

#### **About MJB Technology Solutions**

MJB Technology Solutions is a vendor neutral technology advisor and partner for small to medium sized businesses. With enterprise level business technology services tailored to each company's unique technology challenges and needs, business owners and managers are able to focus on their business and achieve ePeace of Mind™. Learn more at [www.mjbsolutions.com](http://www.mjbsolutions.com).