

microsoft.public.win2000.security: Re: How to best protect computer from massive failure?

## Re: How to best protect computer from massive failure?

*Source:* <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2002-06/2806.html>

---

*From:* x y ([jamescagney90210@excite.com](mailto:jamescagney90210@excite.com))

*Date:* 06/30/02

From: "x y" <[jamescagney90210@excite.com](mailto:jamescagney90210@excite.com)>

Date: Sun, 30 Jun 2002 08:17:57 -0400

I would add to the other poster's comments that an antivirus program such as Norton that was set to download updates daily is probably the best way this could have been avoided, if it was really malicious code.

This may be overkill, but in addition to an antivirus program, you could also consider using trojan scanning software such as [www.pestpatrol.com](http://www.pestpatrol.com) or [www.gfi.com](http://www.gfi.com). This software is often somewhat new, somewhat buggy and sometimes prone to false alarms, e.g. telling you there is a problem where there is none. However, it's probably not advisable to run both memory-resident real-time virus and trojan scanners as one can detect the other as a virus and cause problems. The other alternative if you wanted to run both programs would be to manually scan files that you download before executing them. However, malicious code that is downloaded in a web page instead of as a file download would only be scanned by your antivirus scanner, you would probably not get a chance to manually scan it. I do just fine just running an antivirus scanner without using trojan scanning software.

A software and hardware firewall could have helped detect some malicious code as well, starting with sygate [which is free for noncommercial use] and netgear or linksys NAT router "firewalls" starting around US \$70. I would definitely suggest that using a NAT router to share your DSL is safer than using a Windows 2000 machine. [Without knowing more of the details, I have to wonder if the code was maybe not as malicious as you thought and whether more harm was done by shutting the system off while writes were being made to the hard drive.] Again, if you run Sygate or another personal software firewall, you may need to tell your antivirus scanner not to scan the folder it is installed to.

I'm not sure the partitioning you pick makes much of a difference when it comes to malicious code. Since you have 3 hard drives, you could use Windows 2000 to mirror two of the disks, this helps protect against physical hard drive failure but does nothing to help against software corruption such as malicious code or the computer being shut off while some program is writing to the partition table. Converting your partitions to NTFS may help

Re: How to best protect computer from massive failure?

microsoft.public.win2000.security: Re: How to best protect computer from massive failure?

protect against a few types of problems, though you won't be able to dual-boot to other operating systems that don't understand NTFS partitions.

For other ways to secure windows 2000, follow the checklists at [www.microsoft.com/security](http://www.microsoft.com/security) Especially note the instructions on securing IIS if you are running web or ftp services.

"bry" <[bry@bry.com](mailto:bry@bry.com)> wrote in message news:emGWVI5HCHA.2644@tkmsftngp10...

> *I recently downloaded and installed some malicious code which I realized was*

> *not the update I was expecting. I turned off the system and saved most of everything but have spent a week restoring w2k to previous state. How do*

I

> *minimize this should it happen again. I currently have 3 hard drives.*

Due

> *to past circumstances, my boot drive is 40 Gig drive designated H. I also*

> *have a 16 Gig drive C and 9 Gig D. Is it correct to think that I start with*

> *correct partitioning and layout? And if so, what is best. This computer is*

> *the connecting computer on dsl with two more on LAN.*

> *Thanks*

>

>