



Serving the Financial District for over 38 Years

47 ANN STREET
NEW YORK, NY 10038

Tel: (212) 349-1233 • 349-4545

Fax: (212) 406-7074

Email: nova@novaoffset.com

Web Site: <http://www.novaoffset.com>

The answer to all of your printing needs.



Vol. 6, S-ZZ

Computer Viruses & The Tools to Fix Them

It's every computer user's nightmare: a mysterious message or strange error on the computer's screen that seemingly comes out of nowhere. You check your program, restart the computer, maybe even reload your software, but nothing helps.

What can you do?

If you think that your computer is infected, the first thing you should do immediately is turn it off and unplug it if you have to. Don't go through the normal shutdown procedure and don't wait for the computer to finish any processes it's completing. Just turn it off.

Although turning off your computer, mid-process can also cause some problems, they are minor compared to what some viruses can do if they are left to run.

By the way, if you are reading this and you actually have a virus right now, skip down to the section heading "Emergency Procedures" and come back to this later.

What is a Computer Virus?

Just as weeds are plants in our garden which grow in ways (or in places) we don't want, computer viruses actually

are nothing more than programs that do things we don't want them to do. In your computer, a "healthy" program will perform its tasks without interfering with any of the other programs in your computer. Computer viruses are programs that are designed to harm your computer in one way or another. For example, some viruses delete important files while others create files which keep getting larger and larger to eventually fill up your

"If you think your computer is infected, the first thing you should do immediately is turn it off."

hard drive with useless data.

Viruses also can cause other programs to make mistakes. One that has been reported as a Y2K virus creates date and time errors in other programs and in your system files. It does this to make the user think there is a Y2K bug in the computer so they will begin a wild goose chase, searching for problems that don't exist.

How Does a Virus Get into your Computer?

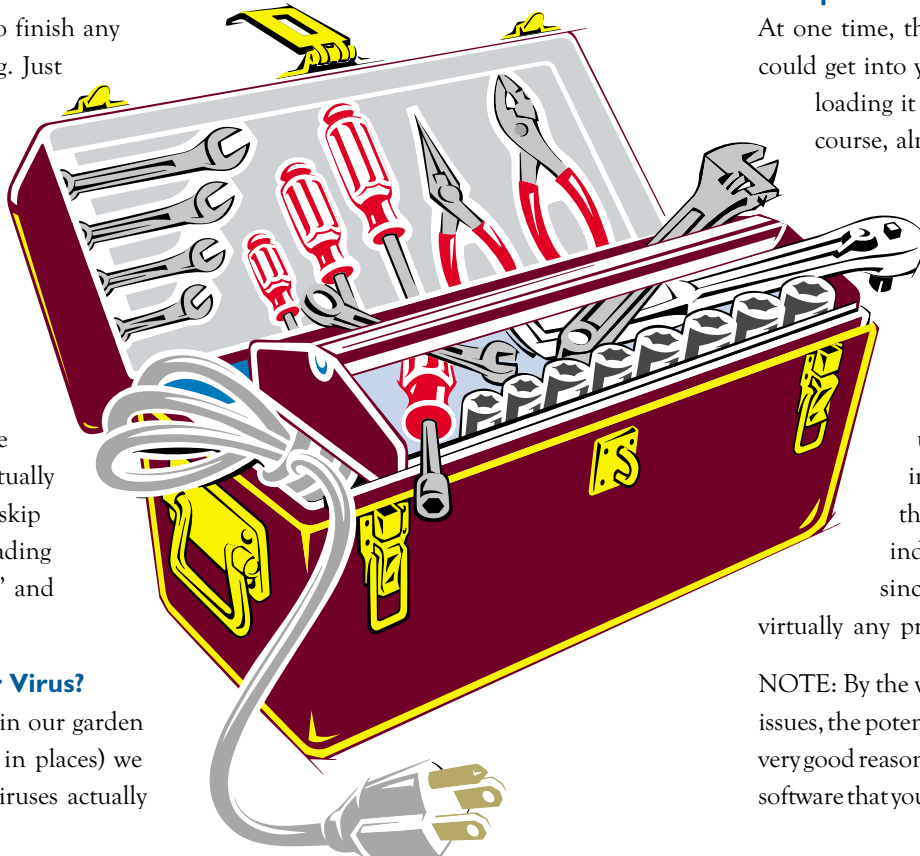
At one time, the only way that a virus could get into your computer was by loading it and running it. Of course, almost no one would

deliberately try to get a virus, so the viruses had to find a sneaky way to make you run them.

Most viruses hide inside other, apparently useful programs. In fact, in their uninfected form, those programs may indeed be quite useful, since viruses can infect

virtually any program.

NOTE: By the way, aside from the legal issues, the potential of a virus infection is a very good reason never to load copies of software that you didn't purchase into



your computer. The copied program may have been contaminated with a virus on its way from the original source to you.

Today, however, there are new ways for viruses to infect your computer. One is used by a special virus called a macrovirus. Macroviruses are usually bundled into documents produced by applications like Word or Excel. Word and Excel (like many other programs today), have the ability to automate certain tasks. To do this they have, built into them, programming commands that can be used to perform complex tasks using anywhere from one to only a few keystrokes or mouse clicks. By hiding in these kinds of documents, the macrovirus can actually open and run itself when you do nothing more than read the document.

There are also email viruses which hide in documents that are designed to be read by programs like Microsoft Outlook. Outlook performs a number of things automatically when it reads your documents and all you need to do to activate some of these viruses is click on them in your email list if you have a mail utility and they will open and run automatically just as the macroviruses do.



Steering Clear of Virus Attacks

According to Symantec, one of the leading producers of anti-virus software, at last count there were between 40,000 and 50,000 known viruses with between 200 and 300 in wide circulation at any given time. That gives you pretty good odds that you'll encounter a virus at one time or another.

The only way to be sure that you'll never get a virus infection in your computer is to never download anything from an unknown source. This means (among other things) that you should never download music, videos, games, or pictures from anywhere on the Internet, since you can't possibly know that the source computer is completely virus-free.

Of course, avoiding all downloads, while possible, is quite difficult these days. The Internet is a very important part of computing today and sending and receiving emails is an essential of the whole process.

What can we do? Viruses are everywhere today and they now have multiple ways of finding their way into our computers.

Perhaps it will help to think of computer viruses as we do human viruses. We are surrounded by them all of the time but we don't get sick every time one of them comes our way. The reason for this is because people have an immune system that protects us from most illnesses. Only a few make it past our defenses and even then, most are eliminated without our ever noticing that we were sick.

Although more and more new systems are being shipped with anti-virus software preinstalled, computers don't automatically have the same kinds of built-in defenses that we do. If your computer didn't have anti-virus software preinstalled when you bought it,

you would be well advised to install it yourself. Without it some kind of antivirus software your computer it will have no resistance to viruses.

Two of the better antivirus programs available are the Norton (Symantec) antivirus and McAfee's. Both are inexpensive and both are generally available in trial versions from their websites. For Symantec the URL is www.symantec.com and the URL for McAfee is www.mcafee.com

Emergency Procedures

If you're reading this, chances are you are facing a crisis right now. If you aren't, you may still want to read this section so you'll know what to do if you find yourself face to face with an ugly virus someday.

The first thing to do once you are pretty sure you have a virus is stop it from causing any more damage [NOTE: Once you notice a virus, chances are, it's already done some damage].

If your computer is operating somewhat normally, exit all of your current applications and shut down the system. If you got a message telling you that your computer is reformatting your hard drive(s) or some other serious threat, don't wait for things to settle down, reach behind the system and turn it off or unplug it immediately. This will stop the virus from doing any further damage.

The next thing you should do is get a copy of a rescue diskette. This is a special "clean" system diskette that is shipped with most antivirus programs. It allows you to boot up your system (you'll usually put the system on from your own computer) from a diskette that you know isn't infected with a virus. Once booted the rescue diskette will direct you to run some tests and will often make all of the repairs to your computer nearly automatically.

A Backup Schedule that Works!

Although most of us never want to ever lose any of our valuable data, with today's huge hard drives, it would be easy to get lost backing up the whole hard drive every day. It would be a monumental task!

Fortunately, most backup systems have a means of doing incremental backups. Incremental backups only backup the data that has changed each day. Each day's backup media is then stored separately until the scheduled full backup occurs. When you run a full backup, you can erase the old, incremental backups and use them for the next period.

With this schedule, full backups

are generally performed every other week. If you need additional security you can do weekly full backups (say, every weekend or every Friday) and keep the most recent weeks' daily media until you run the next full backup. That way, if anything happens to your full backup you can always restore your data from the pervious weeks' dailies.

Regular Security Schedule

M Partial backup #1
 T Partial backup #2
 W Partial backup #3
 T Partial backup #4
 F Full backup (erase weekly backups for use next week)\

Higher Security Schedule

Week #1
 M Partial backup #1a
 T Partial backup #2a

W Partial backup #3a
 T Partial backup #4a
 F Full backup "a" (erase full backup "b" and partial backups "1b-4b")

Week #2

M Partial backup #1b
 T Partial backup #2b
 W Partial backup #3b
 T Partial backup #4b
 F Full backup "b" (erase full backup "a" and partial backups "1a-4a")

Week #3

M Partial backup #1a
 T Partial backup #2a
 W Partial backup #3a
 T Partial backup #4a
 F Full backup "a" (erase full backup "b" and partial backups "1b-4b")

Week #4

M Partial backup #1b
 T Partial backup #2b
 W Partial backup #3b
 T Partial backup #4b
 F Full backup "b" (erase full backup "a" and partial backups "1a-4a")

a vocabulary of the graphic arts

Full Backup: To copy all of the information on an entire hard drive or an entire hard disk partition to another device (usually a removable media device).

Partial Backup: To copy only the information which has changed since the last backup of a hard drive or a hard disk partition to another device (usually a removable media device).

Hard Disk Partition: A virtual hard drive within a hard drive. On some systems the hard drive is so

large that managing the data in one huge block would be difficult or impractical. To make it easier to manage these very large drives, they may be "logically" broken up into smaller "partitions" which appear to the user as additional, smaller drives with their own drive letters.

Computer Virus: A (generally) malicious program designed to infiltrate a computer system and cause data loss or other system damage.

Computer Macrovirus: A computer virus that is embedded in the data file of a program that can use or create macro programs.

Macro Program: A user-defined "program" designed to perform tasks within a larger program. A Microsoft Word Macro might be created, for example, to put your name and address at the top of every personal letter you write.

Antivirus Program: A special computer program designed to find and eliminate computer viruses and the damage they cause(d).

TRICKS & tips

Choosing the right backup media can make a huge difference in preserving your data. At one time the most popular backup medium was floppy diskettes. However at only 1.44MB (million bytes) per floppy, you would need a lot of them and a LOT of time to back up a typical hard drive. Today the average hard drive is at least 4GB (billion bytes). What this means is that if you tried to backup the entire hard drive using floppy diskettes you would need nearly three thousand diskettes! Of course, most of the time hard drives aren't full; in fact, for the best performance you should replace your drive with a larger one or delete a lot of files if your drive reaches 75% full.

There are many choices of backup media, ranging from ZIP and Jaz disks

to tapes and CDR/CDRW discs. Your choice should be made, based upon your system needs. The table below lists some of the features of different backup media. You need to be aware, however, that because the computer industry changes so quickly prices, features and availability can change at any time.

Device	Capacity	Speed	approx. Price (drive/medium)
ZIP 1 drive	100MB per disc	Medium-fast	\$100 / \$11
ZIP 2 drive	250MB per disc	Medium-fast	\$150 / \$18
Jaz 2GB Drive	2BG per disc	Fast	\$350 / \$125
CDRW Drive	650MB per disc	Medium-slow	\$250
CDR Media	650MB per disc	-	\$1.99/disc*
CDRW Media	650MB per disc	-	\$2.99/disc*

* At the time of this writing there were virtually no CDR-only drives so these two listings are for the same drive. The difference is in the medium. CDR discs can be written to only once and are less expensive. CDRW discs can be written and erased repeatedly but cost a bit more.



Serving the Financial District for over 35 Years

**47 ANN STREET
NEW YORK, NY 10038**

**Tel: (212) 349-1233 • 349-4545
Fax: (212) 406-7074**

*Email: nova@novaoffset.com
Web Site: <http://www.novaoffset.com>
The answer to all of your printing needs.*

PRESORTED
FIRST CLASS MAIL
U.S. POSTAGE PAID
NEW YORK, NY
PERMIT NO. 4396