The Technical Side
Computer Viruses

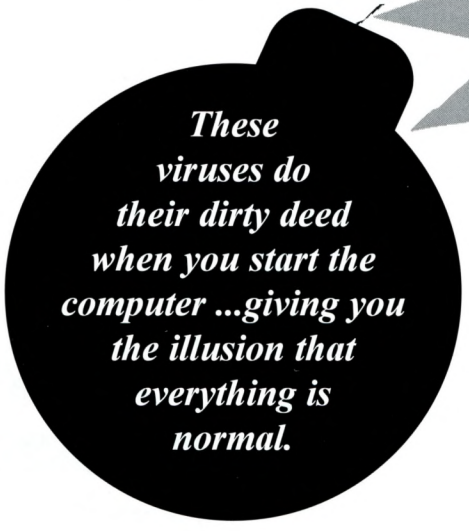
By Chris Cothrun, Ingenuity Inc., Copyright Ingenuity Inc.

We are going to depart from our usual survey-related topic and instead discuss something that affects every computer user: computer viruses. We increasingly depend on our computers to accomplish our everyday tasks. We also share information with other computer users to a greater extent than ever before through networks, the internet, or even the lowly floppy disk. All of these increase our exposure to computer viruses that can cause loss of data and hours of frustration restoring your system. I will provide you with some information that will enable you to lessen the chance of losing anything to a computer virus.

First, I'd start with a disclaimer: I'm not a computer virus expert. I'm going to try to educate you about viruses, but I can't be responsible for what you do if you have or suspect you have a virus. I, of course, cannot be responsible for any damage a virus does. If your computer is part of a larger network, I suggest you consult further with your Network Administrator or someone else in charge of computer policy if you suspect a virus or before changing your computer's configuration.

So, what exactly is a computer virus? Any relation to the microscopic nasties that give you the sniffles? Hardly. A computer virus is simply a computer program with a few special characteristics. Foremost among them is the capability of replicating itself, hence the name. Viruses usually attempt to remain undetected, at least until they have a chance of copying themselves. Beyond that, what the virus does is up to the author. Some stop at making copies of themselves, others annoy computer users, and still others intentionally or unintentionally destroy files. Any of these actions on your computer is most likely unwanted. So what can you do?

You can first take steps to avoid getting viruses and to avoid significant damage if your computer is compromised. You should have a set of boot disks for your computer that are write-protected. These should contain a copy of your operating system to boot the computer, enough disk utilities to restore your computer as necessary, and a virus detection and removal program. A good backup system is important if you wish to minimize the damage a malevolent virus might do. But you must try to avoid backing up the virus along with your data.



You may be familiar with the numerous virus detection programs available for computers. If not, these are programs that scan through each of the programs on your computer and took for virus "signatures," or unique sections of binary data that would identify a virus. Some of the more advanced packages also look for suspicious activity that might indicate a virus is making a copy of itself. Some packages also look for viruses in data coming over a network or internet connection. If you use one of these, you must first make sure you have current updates for the latest crop of viruses. The AntiVirus that is included with DOS and Windows doesn't count as a recent version of a virus detection program. You should rely on something more robust to avoid virus problems. I won't recommend any particular package, but several are available for download and evaluation from sources listed below.

A number of viruses like to hide in the boot sector, the area of disks that the computer goes to when loading DOS, the various flavours of Windows, or any other operating system. These viruses do their dirty deed when you start the computer and then start your usual operating system, giving you the illusion that everything is normal. Many computers are set up to first check the floppy disk drive for a boot disk and then the hard drive. If you accidentally leave a floppy disk in your drive when you boot your computer, this can let the virus copy itself to your hard disk drive. You can guard against this by changing your BIOS settings to boot from your hard disk only.

Another class of viruses takes advantage of the fact that many popular software programs include powerful macro programming languages. The most notable examples were several viruses that used the Microsoft Word macro language and program features to spread. If your organization makes heavy use of Microsoft Word, you should take the time to educate yourself about this virus and the steps to take to prevent its spread.

As mentioned in the introduction, the increased use of networks, online services, and the internet can increase our exposure to computer viruses. How safe is it to download programs, e-mail, and data from these? It depends on the source. All online services scan their file for viruses. Most of the major software archives on the internet also look for viruses in their collections. But other Internet sources may pay less attention to the threat from viruses. Any of these sources are susceptible to new viruses that are unknown to the virus detection programs. Any file attached to mail would be suspect, especially if they are from an unknown or untrusted source. Your safest bet is to scan anything that

you download or receive in e-mail. The Internet also introduces some new computer security and virus risks. The Java and Active X technologies add another way malevolent programmers can gain access to your computer. While there is work being done to prevent these from being a risk, I would advise treating these technologies with caution.

There have been several "Trojan Horse" viruses, or programs that claimed to be a new version or an upgrade of some commonly used software but were actually either virus-infected or simple attempts at deleting the contents of your hard disk. These can be avoided by obtaining upgrades from the company authoring the software. There also have been virus hoaxes, the most notable being the "Good Times" hoax. This consists of an e-mail message warning you about another e-mail message titled Good Times. The message goes on to warn you about the damage that this will do if you download it to your computer and concludes by telling you to pass this message on to everybody you can. The first clue that this is a hoax is the warning to not even download the message. Just like any other program, a computer virus has to be run before anything happens. For nearly all e-mail systems, nothing in a message is run or executed unless you tell it to. If your mail program automatically executes attachments without giving you a chance to scan them for viruses, you need to get a new mail program. If you receive a message warning you about a new virus, don't pass it on until you confirm that it is in fact a genuine warning and not another hoax.

The following online sources are an excellent source of information and discussion.

Internet Newsgroups: alt.comp.virus and comp.virus offer discussion and advice, often from representatives of major virus software manufacturers.

Online service sources include: America Online: Keyword: Virus CompuServe: GO VIRUS. I highly recommend the NCSA Web site. They have tested major virus detection and removal programs and provide lists of certified packages. They also address other issues of computer security. You can find them at: http://www.ncsa.com.

Shareware virus detection programs are available from: http://www.coast.net/SimTel/msdos/virus.

The following commercial web sites contain virus information, including evaluation versions of virus detection packages, information on the latest viruses and the latest hoaxes circulating, and further advice and instructions if you suspect you have a virus: http://www.av.ibm.com/current/FrontPage, http:www.symantec.com/avcenter/index.html, http://www.mcafee.com, http://www.drsolomon.com.

Comments and discussion are always welcome. Please contact us at The Technical Side, 1562 Linda Way, Sparks, NV 89431, fax us at (702) 359 6693, or e-mail us at cothrun@ix.netcom.com. Visit our web site at: http://ourworld.compuserve.com/homepages/cothrun/