A BIT OF VIRAL PROTECTION IS WORTH A MEGABYTE OF CURE

Tim Fitzgerald
Communications Specialist
Computing and Information Services (CIS)
University of Pittsburgh
document@vms.cis.pitt.edu

Even in today's world of safeguarded networks and advanced detection software, computer viruses are still running amok in some of the seedier niches of cyberspace and hiding out on unclean disks and unprotected hard drives. Speculative rumors of wide-spread epidemics have only added to the confusion as computer users all over the world wonder if their systems are at risk and if there is any way to shield themselves from these stealth operatives of electronic malfeasance.

The reality of computer viruses is that they have never been able to live up to their apocalyptic billing. Unfortunately, the actual damage that viruses cause is usually measured on a personal scale. You may think that one infected machine out of a thousand is a good margin of safety until you find out that it was your term paper or thesis that was compromised or lost. For this reason, it is essential that all users of CIS services be aware of the threat of viruses and what measures will keep them from spreading.

Computer viruses may differ in how they are spread and what damage they do. Some take a long time to develop or assert themselves, while others move very rapidly. Most viruses attach themselves to the formatting areas of floppy disks or in executable programs. Some bits of code, such as Trojan horse programs and worms, work so much differently than other viruses that they no longer fit the accepted definition of a virus. The exact definition of a virus changes about as often as a new strain is reported. Perhaps, a computer virus is best defined as "a piece of computer code that hides in places where it should not be, replicates itself gratuitously and then travels to places where it should not go in order to do things that no one wants it to do." Although virus detection software is available to screen for viruses and disinfect disks, the constant introduction of new strains means you should never rule out the possibility of a viral infection, even on well protected systems such as the computers in the CIS computing labs.

Viruses seem to subscribe to one of Murphy's little known corollaries on computing: a computer virus will manifest itself at the worst possible time in relation to each individual user's case. This usually happens an hour before a paper is due, when the lab is about to close or any time late in the term when there is no time to start a project all over again. Even with scrupulous preventative measures, some nefarious programs may still slip past these defenses and cause great damage. You should always be aware of this possibility when experimenting with strange disks and new applications and always remember to back up whenever you think that your system may be placed at risk.

While it is important to acknowledge the threat of computer infection, there is no need to scrap your disks and move all your work back to paper, pencil and adding machine. If you practice simple, common sense procedures of safe computing, then your chances of being victimized by a virus are relatively slim. Most preventative procedures, especially at the floppy disk level,

take very little time and could save you a lot of time and invaluable personal effort, even if you should come in contact with a strain.

A simple fact to remember about a computer virus is that you do not want one and modifying your behavior is one of the best ways to avoid one. Since most viruses are hidden in programs, you should be wary of executable files or applications from places that you cannot trust. If your disk or system should contract a virus, do not panic, but get rid of it as soon as possible since it is impossible to determine how fast a virus will work or how much damage it is capable of causing.

The worst thing that you can do with regard to computer viruses is nothing. Just because you haven't heard of a viral outbreak does not mean that the coast is clear. The very nature of viruses is to slip in unnoticed, very quietly go about the business of reproducing and do selective damage.

You can combat computer viruses actively and passively. To take an active approach to the problem, you should check out the many software packages available for both the Macintosh and DOS computing platforms. If you do all of your work in the CIS labs, you do not need to investigate this software since the computers in the labs are already well equipped with the latest programs to detect and eradicate viruses. If you are running a system from your home or office, you should be aware of the many different packages and the options they feature. Information about popular anti-virus software is included at the end of this article along with directions for obtaining copies of free software.

Passive protection against viruses requires nothing more than observing and maintaining good habits of safe computing. The practice of safe computing involves a general wariness of strange disks and programs downloaded from Internet, anonymous FTP or outside bulletin boards. Also, the spontaneous and casual disk swapping that characterized the early days of the personal computer revolution must now become a thing of the past. While you may value your friends, you should not hesitate to scan their disks before running their files. A good rule to follow is, "When in doubt, scan."

Backing up your work is also another common sense procedure that all CIS users should put into practice. Back up anything that you would not want to lose. Following a schedule of regular backups will minimize the harmful effects that you may suffer from viruses as well as collateral damage from mistakes and other unforseen problems.

Diagnosing Viruses

Often, a good way to detect the presence of a computer virus is through subtle changes in the speed of your computing. Since most viruses move very slowly, they will not adversely affect your work until they have had time to grow and expand. Trust your instincts in regard to viral suspicions. If a file seems to be taking an increasingly long time to load every time you use it, you may want to check the file or the disk for a problem. This is especially true if you are not adding a lot of text or graphics every time you access the file. If you are running your own system, you may notice that an application or a file taking a bit longer to load than usual. If you know your system well, then you should be able to detect when an application is taking too long. Viruses will also affect disk directories. Both the Macintosh and DOS environments allow you to check file sizes and dates. If a file has a modified date or is larger than you remember, then a virus might be present.

Disk viruses will often disable a disk's functionality by expanding so far into the formatting area that the disk can no longer produce a directory. The DOS system will produce a standard "Error reading Drive A" message, while the Macintosh operating system will call a disk unreadable. If this message pops up while you are working, do not hit the panic button that reformats the disk. Each CIS computing lab has a virus detection station that can find and clean infected disks without wiping out all the work stored on the disk. The

CIS disk repair service at G-27 Cathedral of Learning can also fix a virus-damaged disk. If you are running a system at home, certain utility packages that you can buy at the PC Center — such as Norton Utilities for Macintosh and DOS — can fix areas damaged by a virus. These packages, however, should not be used as a substitute for an up-to-date virus detection program.

Avoiding viruses in the computing labs

The CIS computing labs have many defenses against computer viruses. However, it is still possible to pick up a virus from a lab machine if you aren't careful. The easiest way to pick up a virus is to begin working on a lab PC that is already running. Some viruses hide out in active memory where even the best scanning software can't find them. Of course, these types of viruses will be wiped out as soon as the PC is shut down and then restarted. CIS has always recommended that you restart a lab PC before attempting to use it. This will clear the machine's active memory and re-invoke the protection software guarding the network and hard drives. Also, you should always shut down your PC after you are done using it. This reduces the possibility of spreading a virus and ensures that your Network Authorization Account privileges cannot be accessed by the following user.

The DOS-based machines in the CIS labs use the PC Guardian program to protect against viral infection. Infecting the hard drive of a PC in the lab or the network file server is impossible since all of the drives and the server are read-only. PC Guardian, however, will still display an alert if a virus should attempt to write itself from an infected disk onto these locked areas. If a message like this should appear on your screen, then you should take that as a clear indication that something is amiss. You should save your file and exit your application immediately, restart your machine and then use the lab's virus scanning station or the ViruCide program to scan and clean all of your disks. ViruCide is available under the "Utility/Printer" DOS Application Server menu.

The Disinfectant program on the Macintosh machines exists in both application form and as an INIT so it is a bit more pro-active than its DOS-based counterparts. Like the DOS environment, the Macintosh hard drives and server are locked and will not allow anything, including a virus, to be written there. If you get a Disinfectant message or a strange disk error, you should save and exit your application immediately, restart your machine and then use the virus scanning station or the Disinfectant application to scan and clean all of your disks. The Disinfectant application is available in the "Virus Protection" folder under the "Mac Applications" server icon.

If you are lending a disk to a friend to copy a file, slide the black tab in the upper right corner until the square opening is not blocked. This is the disk's write-protect tab and, when it is slid open, nothing can be written to the disk. Sliding the tab closed produces an at-risk disk that software applications and viruses can write to. Five and 1/4 inch disks need to have a write-protect sticker placed over the notch on the side of the disk in order to be protected.

Avoiding viruses on your home or office machine

In order to feel secure on your home or office PC, you should minimize the risk of contracting a virus from an outsider and equip your system to handle any possible intrusions. You may want to invest in a good anti-virus software package that has many different options. Some scanning programs will automatically check any disk that is placed in a floppy drive. These involuntary scans may slow you down if you do a lot of disk swapping but will definitely enhance the security of a system that is frequently exposed to outside disks. All of your source and backup disks should have their write-protect tabs enabled.

You should print a paper copy of your hard disk directory that lists all of your software application files along with their original size and date. This way you can quickly check to see if any application files have grown in size or have modified dates. This hard copy listing should be

updated every time you add a new software application to your system.

If you really want to try out an unfamiliar program or read a strange disk, you should at least use a virus scanning utility before running any of the new programs since most viruses are transmitted by running the host program or hooking onto the disk directory. Viruses hiding in the formatting areas of floppy disks cannot write to memory until the directory command is given. This is why you should scan outside disks even before finding out what files are on them. With many viruses that hide in applications, you can load an infected program onto your system but the virus will not be transmitted until the program is actually run. If you scan all new programs before running them, you can delete any infected files before they can do any damage.

Avoiding viruses from VMS, UNIX or USENET

Viruses on the VMS and UNIX Timesharing Services, as well as the UNIX-based workstations in the CIS computing labs are not as common as PC-based viruses since only a few CIS personnel have the privileges to write to the system areas of these machines. However, it is still possible to contract a virus that will affect your personal directory. The only way that this is possible is if you download an infected executable image and then run that image on your personal disk area. In this case, only your disk area would be affected by any viruses.

A virus could not spread to the directory of another user unless that user copied the infected image to his or her directory and ran it there. A VMS or UNIX-based virus could never spread to the system files unless a VMS or UNIX administrator with appropriate privileges copied the infected program and ran it on the system level. This is highly improbable, however, since no competent systems professional would run an unknown program without checking it out first.

The UNIX-based workstations in the CIS labs are protected from viruses in the same way as the VMS and UNIX Timesharing Services. That is, the limited privileges for the systems areas of these machines make it impossible for a virus to be spread through the general computing community.

Catching a virus through e-mail or USENET

You cannot contract a virus through electronic mail; that is, no one can send you a poisoned e-mail message that will do damage once it is received. The only way that you can contract a virus through e-mail is to receive the ASCII code of a program containing a virus and then compile that code on your disk area. A UUENCODEd binary image received through e-mail could also contain a virus, but the virus would not be able to activate until you ran the actual program.

Since most postings to USENET are plain text ASCII files, the likelihood of getting a virus from a news group posting is rare. As with e-mail messages, only a binary image of a program can spread a virus to your system. GIF files and other graphic files transferred in binary format cannot spread viruses since they are read but not executed.

Obtaining free anti-viral software

The Office Systems Services Group of CIS (OSS) recommends the Disinfectant program for Macintosh PCS since it is available free of charge and is updated regularly. Free copies of Disinfectant are available in the "Virus Protection" folder in the "Mac Applications" server on the Macintosh PCS in the CIS computing labs. Disinfectant is also available at the PC Center and via anonymous FTP at the address acns.nwu.edu in the /pub/disinfectant folder. Other Macintosh anti-virus programs of note are SAM, Gatekeeper and Virex.

For DOS-based PCS, OSS recommends F-Protect 2 software. OSS has obtained a site-license for this software so that all students, faculty and staff may obtain a copy free of charge. To receive a copy of F-Protect 2 or Disinfectant, bring a disk to the PC Center and they will copy the software for you. Visit the PC Center at 204 Bellefield Hall, 315 South

Bellefield Avenue, open Monday through Friday from 10:00 a.m. to 4:00 p.m., 624-1380.

Other anti-viral programs for DOS-based PCS include Norton AntiVirus, Microsoft AntiVirus and McAfee VIRUSCAN. OSS has compiled two charts (see hard copy) that compare the features of these Macintosh and DOS-based anti-virus programs.

Tips for Avoiding Viruses

- Backup your work often. If you work in the CIS computing labs, use two disks in case one of them should become infected.
- Never do a disk directory on an unfamiliar disk without scanning it first; scan all new programs as well.
- Be aware of the risks of swapping or downloading programs from bulletin boards.
- Keep a hard copy of your disk directory to better detect files that may have been altered by a virus.

Teaching an Old Bard New Tricks: Shakespeare Interactive Archive

Lee Ridgway
Senior Technical Writer
Publication Services
Massachusetts Institute of Technology
ridgway@mit.edu

The Shakespeare Interactive Archive is the rather unassuming name of a multimedia project whose ambition is to be a model for the future in Shakespearian studies. Its creator, Peter Donaldson, Professor of Literature, envisions this computer-based project as a comprehensive, international archive that networks as many libraries and resources as possible. Textual, visual, and moving image files would all be linked.

Act I, Scene I

Donaldson's start on the project was a more modest and specific idea: to take all the films of Shakespeare's plays published on laser disk and link them to the corresponding printed texts; and to create software that would get you from any line in a play to the corresponding spot in a performance, in as many performances as possible. The germ of this idea goes back to 1969, when Donaldson began teaching courses on Shakespeare at MIT.

Wanting to expose students to performances of Shakespeare, Donaldson would show complete films of plays in the evenings. This proved frustrating because it added two or more hours to students' already long days - not the best circumstances under which to enjoy the films and get something out of them. Donaldson also found that this was not a good method for how he wanted to teach Shakespeare.