

Virus Checker

August 2001

To Prevent the Spreading of a Virus

The only way to prevent the spreading of a virus is to check your disk before and after using it on a public computer. The GSU campus has a site license for Norton's Anti-Virus Toolkit, and you can find the software on any of the computers in the library.

To Know When You Have a Virus

If you are using a computer at the Henderson Library, you will know you have a virus when a Norton AV alert box appears on the screen.

To Clean a Virus

Double click the Anti-Virus icon on the Windows 95/98 Desktop. Select Scan A Floppy. Check the box relevant for your disk 3½ floppy (A) or Removable Disk (G) for your zip disk. Click the Scan button. Norton's will scan your diskette for any known viruses and attempt to delete the virus if possible. If for some reason Norton's is unable to delete the virus, it will quarantine it. If you have problems refer to an assistant at the Help Desk. Keep in mind that virus software should be updated regularly to keep up with new viruses that are being created or written.

Common Misconceptions of Viruses

(Taken from a paper written on computer viruses and found at: <http://www2.ncsa.uiuc.edu>)

Misconception #1: Computer bulletin board software should be avoided because BBSs are a leading source of computer viruses. The fact is that the most common viruses (the boot track type) could not possibly be either loaded to or down loaded from a bulletin board by any normal or accidental means. Of the computer viruses which could move this way, most simply do not. Bulletin board operators and users are actually a very conscientious lot. This means that any policy against using modems, bulletin boards, public-domain software or shareware, will have no significant benefit in reducing an organization's virus problem.

Misconception #2: Software piracy is the leading cause of virus spread. Viruses travel more with program diskettes than with data only diskettes. The fact is that boot legged software does contribute to the virus problem, but the much more significant contributor is diskettes which contain only data (or even no data like blank formatted diskettes). Although it is true that computer viruses cannot infect data per-se and survive to reproduce, the most common viruses can and do infect the diskettes carrying only data. And when those diskettes are used, the virus can infect the next computer's hard drive or files.

Misconception #3: Most viruses intentionally cause damage by erasing files, formatting disks, etc. The fact is that most viruses do not intentionally cause any explicit damage. And even the viruses which are programmed to trigger a damaging activity almost never cause harm by this programmed activity. This is because most virus instances are discovered before the programmed "trigger date." Once discovered, the real costs of computer viruses come into play -- the work in trying to find all instances of them in your computer and at your site, and in trying to remove them and de-contaminate the computers, disks and programs that the viruses have infected.

Misconception #4: There are good viruses and bad ones. This is a very common misconception. Those who write and distribute computer viruses commonly claim that theirs is a "benign" virus because it has no malicious trigger event and does no intentional harm. They are duped by the same set of misconceptions that have duped the rest of us -- that the problems computer viruses cause are mainly due to the trigger events. In fact, because all viruses replicate without the computer user's or owners' knowledge or consent (by definition), the very act of replicating is an act of contamination and is itself harmful. It is much like cancer. The cancer cells themselves are normally not harmful or poisonous, but the fact that they keep growing and cannot be easily discerned or separated from the non-cancer cells makes finding and getting rid of the invasion particularly difficult.

Misconception #5: The virus problem waxes and wanes every few years. Despite the fact that the news about computer viruses comes in waves (mainly the Friday the 13th - Columbus day wave in October 1989, and the Michelangelo wave in February / March 1992), the computer virus problem has grown rather steadily and predictably since it began. During the Michelangelo "crisis", 95% of problems that users experienced from computer viruses were

actually (and predictably) caused by virus strains other than Michelangelo!

Misconception #6: Computer security is effective against computer viruses.

One would think that the reason we have so many computer viruses is that our computers are not "secure". In fact, traditional computer security - that is computer secrecy including access controls and encryption, have almost no effect on computer viruses. During Desert Shield, a significant part of our own command and control network (a quite "secure" network, as you might imagine) was, in fact infected by the then most common computer virus. The virus, called Jerusalem, works quite well in a system where everything is encrypted -- it too becomes encrypted, and only becomes un-encrypted when it needs to infect something.

Misconception #7: Another common misconception is that the computer hardware manufacturers or the computer operating software vendors ought to provide us with systems which cannot become infected. The fact is that computer viruses are just computer programs. Computers are designed to run computer programs. And there is nothing universal about computer viruses that would allow them to be distinguished in advance from any other program. Then we arrive at the unfortunate truth that -- computers are made to run computer viruses! Although it is possible to make it more challenging for computer virus creators, it is not possible to make a virus-proof computer (unless we do not let that computer run any new programs).

Win '95, OS/2, DOS and even Windows NT systems are all easily and equally infected by the dozen most common computer viruses. It is true that some of these operating systems inhibit the replication (spread) of some viruses, but many current computer viruses operate "well" in all of these systems. The newest versions of DOS and Windows including Win '95, DOS 7, and Windows NT do not and will not include any anti-virus software or utilities. It will be completely up to the user to deal with the computer viruses problem.

Other Places to find Information

http://www.qub.ac.uk/csv/software/pc/nav/v_about.html

<http://www.hk-lawyer.com/1999-6/June99-73.htm>

Search an Internet search engine (i.e., Google) for misconceptions computer viruses