

8 July 2005

10 Cardinal Rules of Virus Prevention

Rule #1

Make sure that there is an anti-virus program loaded and running in your system. Take up the responsibility of updating the signatures yourself instead of expecting the manufacturer to do it. After all, you are going to be using it. Auto-updates are not very reliable.

Rule #2

Anti-virus solutions are very affordable, considering the amount you'd spend in dealing with an actual virus attack. You can choose amongst Indian solutions like SmartDog, QuickHeal and Fire Antivirus. If you're keen on foreign ones, then AVG and InoculateIT are available in free Personal Editions.

Rule #3

Avoid downloading and installing every piece of software available on the Internet, as it might prove detrimental to your data. Some Beta programs contain lethal bugs that could corrupt your data.

Rule #4

Be very careful when downloading software offered through newsgroups and e-mailers. Some viruses provide intruders your password and thus access to your system. This can result in file deletion and sometimes even a change in your password.

Rule #5

Steer clear of hacker and cracker sites as though they were infected by the plague. Most of these are infamous for dirty tricks and carelessness. Viruses, Trojans and worms are highly prevalent among posted software.

Rule #6

"Too good to be true" programs such as discounted software, or programs that claim to be free or guarantee free calls from anywhere in the world shouldn't be used or run. Sometimes these links can take you to sites that you'd be embarrassed visiting.

Rule #7

Ensure that you have an Emergency Boot Disk (EBD) for your Windows OS. Make sure that your system is virus-free before you make this disk or else future boot-ups will contain a virus.

Making an EBD is simple. To create a startup disk, open Control Panel Add/Remove Programs. In the Properties dialog box, select the Startup Disk tab and click Create Disk. Follow the onscreen instructions. To create a Startup Disk, at least three brand new, clean floppy disks of 1.44MB capacity are required. Label the disks very clearly after locking



TenStep Supplemental Paper

the write-protect tab. For added safety, try removing the tab without damaging the disk cover.

Rule # 8

Most antivirus programs let you create a virus rescue disk, which is a bootable disk containing system files and a basic version of your anti virus program that runs from the DOS command prompt. The utility of this disk (space willing) can be increased by including FDISK.EXE, FORMAT.COM, DOSKEY.COM, XCOPY.EXE, XCOPY32.EXE and EDIT.COM files. Make sure to label this disk too. Remember to lock the write-protect tab.

Rule #9

Configure your anti virus software to scan every file downloaded from the Internet. For extra safety try and set it up (if available) to scan incoming email too. Certain programs also let you scan Java and ActiveX control. They even prevent access to pre-determined and user-specified Web sites.

Rule #10

Unless you're very sure of a file's integrity, don't use the File Transfer Protocol (FTP) to download files from an unknown site (unless it's your password-protected personal or company site). Even when you download files from your password-protected sites put them in a separate folder (labeled FTP_Down). Take care to scan them before use.

Try not to download files from a remote site's /incoming/folder, as these files have (probably) not been cleared by the administrator and might have something malicious in them.

Finally, do backup your data every week either to floppies (if you have the patience), to CD-R or CD-RW (in case you have the hardware). Alternatively you could just zip up (compress) the important data files and store them on online drives like MyDocsOnline, Driveway, x-drive or i-drive. It's better to be safe than sorry.