

Ten Rules of Common Sense Computing and Virus Defense

If you follow a few simple guidelines, the risk of a virus attack can be reduced to practically zero.

1. **Use common sense when working with external media.**
 - Always scan floppy disks and CD-ROMs that have been used in another computer for viruses before using them in your computer.
 - Write-protect floppy disks before inserting them into other users' computers.
2. When downloading from the Internet, **ALWAYS** scan the files before opening or running them.
3. **Shut your computer down** when you leave for the day to prevent unauthorized use in your absence.
4. **Make regular backups of important files and folders.** Store your backups in a separate secure space, one that is preferably not on your computer. If a virus destroys your files, at least you can replace them with your back-up copy.
5. **Regularly scan your machine for viruses.** Make sure that the virus protection software on your computer is regularly updated to better defend against new viruses.
6. **Use care when reading e-mail.**
 - It's okay to simply open e-mail messages. You can't get a virus from e-mail text.
 - When possible, avoid e-mail attachments when sending and receiving e-mail. When e-mailing documents paste the text from the document into the body of your e-mail whenever possible. If you get an e-mail with an attachment from someone you don't know, delete it.
 - Any e-mail you weren't expecting should be treated with suspicion, especially if the subject line and attachment names don't make sense, **EVEN IF IT COMES FROM SOMEONE YOU KNOW!** Many viruses spread by automatically sending themselves to the addresses found in the victim's address book, and they often include something in the message body that looks like a personal message from your friend (this is called spoofing).
 - Ask yourself the following questions when faced with an attachment: Were you expecting it? Is it a file format that I normally use? Does the file name make sense? If you need to look at attachments, save them to your hard drive first and then use the virus scanning software to check them.

- When you receive e-mail advertisements, do not open attachments in them or follow web links quoted in them. Do not forward or reply to chain e-mails. These types of e-mails are considered spam, which is unsolicited, intrusive mail that clogs up the network.
 - Never open e-mail attachments with the file extensions SCR, EXE, COM, BAT, VBS, SHS or PIF. These extensions are almost never used in normal attachments but they are frequently used by viruses and worms.
 - Never open attachments with **double file extensions** such as NAME.BMP.EXE or NAME.TXT.VBS. Although image, music and simple text files cannot be infected with a virus, viruses can be disguised as these file types.
 - Do not trust the icons of an attachment file. Worms often send executable files which have an icon resembling icons of picture, text or archive files to trick the user into opening them.
7. **Configure Windows to always show file extensions.** In Windows 2000, this is done through Explorer via the Tools menu: Select Tools > Folder Options > View and uncheck "Hide file extensions for known file types". This makes it more difficult to for a harmful file (such as an EXE or VBS) to masquerade as a harmless file (such as TXT or JPG). Windows default setting is to hide the file extension (the last three characters) when filenames are displayed.
8. **Any virus warnings or hoaxes should be sent to the Administrative Computing Helpdesk who can confirm whether or not they are genuine.** Do not forward these warnings to anyone else. While you may think you are warning others about the latest threat, you could be sending them a hoax or altered or incomplete information. Keep informed about hoaxes.
9. **Do not panic if you think you have been infected with a virus.** Perform a virus scan on your computer using InoculateIT. If the scan shows infected results, inform the Administrative Computing Helpdesk immediately and wait for further instructions.
10. **If in doubt, always ask the Administrative Computing Helpdesk for advice.**