

Online Safety 101

Use anti-virus software

Install anti-virus software on every computer you own or use, and make sure they are up to date. New viruses can spread extremely quickly, it is important to have your anti-virus software updated daily.

Set your e-mail filtering

- **Block file types that are often virus carriers***
these include EXE, COM, PIF, SCR, VBS, SHS, CHM and BAT file types. It is unlikely that you will ever need to receive files of these types from the outside world.
- **Block any file with more than one file type extension***
some viruses attempt to disguise their true executable nature by using "double extensions". Files such as LOVE-LETTER-FOR-YOU.TXT.VBS or ANNAKOURNIKOVA.JPG.VBS may appear to be ASCII text or a harmless graphic to the inexperienced.
- **All executable code sent to your mail.montclair.edu e-mail account should be checked and approved**
If unsure of the validity of the attachment forward the e-mail to your local technical team for analysis, however do NOT open the attachment.
This serves two purposes. First, your IT department (or person) can confirm not only that it is virus-free, but also properly licensed, unlikely to conflict with existing software applications, and is suitable (for instance, not pornographic). Second, IT will always know what software is installed on which computers.

*** If you can't filter your e-mails by attachments, make sure you delete all of them with the above mentioned extensions.**

Stay informed about the latest virus threats

Subscribe to Sophos' mailing lists (<http://www.sophos.com/virusinfo/notifications>) for up-to-date information on the latest virus threats, support information, and new product developments.

Protect your computer with a firewall

Computers connected to the outside world should be properly protected from internet threats via firewalls. Laptops and remote home computers should be included; they will also need firewall protection and might not be able to take advantage of a central firewall inside our campus.

Stay up-to-date with software patches

Many software vendors issue advisories on security issues. For instance, Microsoft runs a mailing list (<http://www.microsoft.com/technet/security/bulletin/notify.asp>) which warns of security loopholes and issues found in Microsoft's software and advises on patches which are available for protection. Most vendors provide automatic patch updating for home users.

Back up your data regularly

Make regular backups of important work and personal data, and check that the backups were successful. You should also find a safe place to store your back-ups, perhaps even off-site in case of fire.