INSTRUCTIONAL COMPUTING & INFORMATION TECHNOLOGY

Engage the Students. Infuse the Curriculum.
Empower the Faculty. Enhance the Administrative Process.

Good Practices for Safe Computing

Nothing can keep your computer or your data 100% safe, unless you never use it--but following these suggestions will help decrease your risk.

Never, ever give out your password.

Don't share it with your boyfriend or girlfriend. Don't share it with your best friend. Don't share it with your parents or your sibling. Don't send it in email, *especially* if you've just received an official-looking message asking for that information—those are scam attempts! And, just as a safety measure, change your password every six months or so. (This doesn't just apply to your Hunter NetID password or your CUNY Portal password; you should treat any password you have with the same care.)

Be careful where you use your password.

Many account compromises at Hunter occur when a student logs into a web site from a public computer and then walks away without logging out. Always make sure to log out before you step away from the computer, even if you're only going to be gone for a few minutes. Also, be aware of the people around you; just like with bank card PINs, sometimes passwords are stolen by "shoulder surfing". And, finally, be very careful when using a computer in a completely public location, like an Internet cafe. Always change your password after using it in an untrusted environment.

Run anti-virus software.

Any member of the CUNY community may download Symantec anti-virus software for free from the CUNY eMall. If you prefer a different anti-virus package, feel free! But you should make sure to have some up-to-date, industry standard anti-virus software running on any computer you use.

Keep your computer up to date.

Don't be caught in last month's versions—someone's exploiting them! Set your computer to automatically check for updates for your operating system, your anti-virus software, your web browser, and any plug-ins or other applications (such as MS Office, Adobe Reader, Flash, and Java). Once a week is not too often.

Take care where you stick your drives.

A relatively recent development in malicious software is the USB virus, which is spread by copying itself from an infected computer onto a USB flash drive plugged into it, and then is automatically run on the next computer the drive is plugged into. Make sure that any computer you use a portable drive with is running up-to-date anti-virus software...and if it's not, make sure you get your drive scanned before you use it on any other machine. (The Student Help Desk can scan your USB drive for you.)

"Oh no! I have a virus!"

If you have an anti-virus program installed, immediately run a deep scan of all files and folders. (This could take a while.) Hopefully it will find and quarantine the problem. If you don't have an anti-virus program, immediately download one—but be warned! Some viruses will prevent you from going to common anti-virus websites. If that is happening to you, or if your anti-virus program can't get rid of it, you may need to contact your computer's manufacturer (if it's under warranty) or get an outside consultant to help you. (Unfortunately, the Help Desk cannot assist with student-owned computers.)