Safe Computing Practices

For those working off-campus, here are a few reminders about safe computing practices designed to keep computers and the CTX network secure and virus-free.

Concordia Computer Maintenance

- **Windows Update –** Taskbar pop-ups (near the clock) indicate when updates are available. Many updates are security-related and must be installed to keep Concordia free from hackers, viruses, and malware.
- **Sophos Anti-Virus definitions –** Sophos automatically updates when connected to a network. If the blue shield has a red "X," Sophos needs updating. Double-click the shield when connected to the network via VPN to force an update. If the red "X" persists for more than a day, contact the Helpdesk for support.
- **Software –** Other pre-installed software on Concordia computers may request updates: Flash, Firefox, Java, Adobe Reader, iTunes/Quicktime, RealPlayer, etc. Many programs also have auto-updaters similar to Windows Update.
- **Routine Maintenance –** Run Disk Clean-up and Disk Defragmenter about once a month to help keep computers working properly. Run these programs under the install login.

Prevent Viruses from Spreading

1. **Surf safely**
   a. Do not download software from unknown sites
   b. Scan files for viruses after downloading but before opening
      i. Save file to the desktop, *right-click* on file, select *Scan with anti-virus*
   c. Regularly clean cookies out of browsers
2. **Read e-mail safely**
   a. Do not open attachments until scanned for viruses
      i. Save file to the desktop, *right-click* on file, select *Scan with anti-virus*
   b. Do not sign up for outside e-mail lists unless it pertains to professional work
   c. Avoid HTML e-mail (it looks prettier, but it can also transfer viruses)
3. **Prevent the spread of viruses: if a computer is suspect of infection,**
   a. Disconnect from network and Internet (disable wireless connections)
   b. Run a virus scan
      i. *Right-click* on the Sophos shield in the taskbar, select *Open Sophos Anti-Virus*, select *Scan my computer*

Other Resources for Safe Computing Methods

http://www.staysafeonline.info
http://safecomputing.ttu.edu/
http://onguardonline.gov/docs/stopthinkclick.pdf

Work from Home

Designed to help you be productive at home

CONCORDIA UNIVERSITY TEXAS

Working Off-Campus with a Personal Computer

Webmail, Blackboard and MyInfo are accessible off-campus. Network shares, the "H" Drive, Banner, and Outlook e-mail access are not avail-able off-campus on non-university owned & supported computers.

Security

Physical Security

Use at least three levels of physical security around the computer.

- Use a laptop cable lock to secure to furniture that is difficult to move
- Never leave laptop unattended in public areas, even for a few seconds
- Store out-of-sight in a locked area
- Secure in a locked cabinet
- Theft-deterrent label on laptop

Data Security

Use various forms of security to protect information on the computer.

- Password-protect hard drive
- Encrypt "My Documents" folder
- Store documents that contain sensitive data on the "H" drive
- Separate login for installs
- Lock desktop when not in use
  - *Ctrl+Alt+Del*, select *Lock Desktop* or
  - *Windows key + L*
- Set screensaver to lock desktop in 10 min. or less

Don't forget to regularly back up local files and documents. The "H" drive incorporates redundant features and is backed up regularly. This is a good location to keep your information safe. Copying files with Personally Identifiable Information to a USB flash drive or CD removes encryption and must never be done unless the media (CD/drive) is immediately and properly secured.

Contact the Helpdesk

Website: http://helpdesk.concordia.edu
E-mail: helpdesk@concordia.edu
Call: *512-313-HELP (4357)*

Phone and Voicemail

Phone

Those with university owned & supported laptops may have a software version of their desk phone (called a "soft-phone") installed on request. Contact the helpdesk for more information.

Voicemail

1. Call the voicemail system: 512-313-3001
2. Hit the * (star key), then your five-digit extension followed by #
3. Enter your voicemail password and #
4. Follow the voicemail prompts.

Computer Login

Log in using the same method used on campus. The separate install login is required to install printers or software. Contact the Helpdesk for assistance.

Accessing the Internet

High Speed Internet Access

- A CTX laptop with Internet access can connect to the Concordia network through VPN (See VPN Access).
- If the Internet works, but not VPN, the router may not be configured to allow VPN traffic. This can be changed through the router's administrative interface. The setting is typically called "IPSec Passthrough," but can vary. Consult router documentation for instructions on allowing VPN traffic.
- If the router also provides wireless access, consult the documentation for restricting access to the router through WPA network authentication and/or MAC address registration.

Free Wireless Internet

Below are websites that show where wireless Internet is available in Austin. Sites are reported by users and may not be up-to-date.

- http://ilovefreewifi.com/austin/
  - largest list of wireless-accessible sites
  - includes a map for each site
- http://www.austinwirelesscity.org/hotspot-list.php
  - lists quality of signal at local sites

Be aware that the Cisco VPN client may NOT work from all of these locations. Some locations block VPN traffic due to security. Contact the establishment directly to confirm wireless access and to determine if there are any VPN restrictions.

Printing

A connected VPN will allow printing to campus network printers and copiers.

Network Storage Access

Access to personal network shares and folders is created automatically on-campus. The directions below are for off-campus access.

Personal Folders on the "H" Drive

To connect to personal folder on the "H" drive:

1. Connect using *VPN*
2. Open *My Computer*
3. In the address line near the top type on of the following:
   a. *\\concordia\h_drive\firstname.lastname* - OR -
   b. *\\concordia\h_drive\data\firstname.lastname*

Departmental Shares on the "H" drive

To connect to the departmental share on the "H" drive:

1. Connect using *VPN*
2. Open *My Computer*
3. In the address line, type the following:
   a. *\\concordia\h_drive\data_departmentshares*

Select the 3-letter department code. Contact the Helpdesk with questions about respective department codes.

VPN access

VPN (Virtual Private Network) directly connects users to the Concordia network.

Requirements:

- Laptop must have an Internet connection
- Broadband is best, but dial-up will also work

Benefits:

- Outlook e-mail access
- Network storage access
- Print to network printers
- Secure connection to Concordia

How Does VPN work?

VPN creates an encrypted tunnel through the Internet to the Concordia network.

Connecting to Concordia via VPN

An Internet connection is required. VPN software is installed by request on Concordia owned laptops only.

To run the VPN software:

1. Open the VPN software by going to *Start > All Programs > Cisco AnyConnect VPN Client > Cisco AnyConnect VPN Client*
2. Type "66.193.242.7" in the "Select" box and click "Connect."
3. When prompted, enter your network username and password.
4. The AnyConnect client will minizmize to the system tray automatically once connected.