Computer Security
Do’s and Don’ts for Connecticut College staff and faculty
**Objective**

“To ensure that users are aware of information security threats and concerns, and are equipped to support organizational security policy in the course of their normal work.”

-ISO 17799/BS 7799 code of practice
Why is this training mandatory

- Compliance with recent legislation regarding the handling of sensitive personal information*
- Many of us deal with sensitive/confidential information
- The Internet is a dangerous place
- Computer software is vulnerable
- Identity theft is a serious problem

* Failure to comply with this can result in legal and/or financial repercussions to the college or employee
Things To Worry About

• Is my data secure?
• Is my computer secure?
• Is the network that you’re using secure?
What Are The Threats?

- Lost/Stolen Computer
- Hackers, identity thieves
- Viruses, Worms, Trojan Horses
- Keystroke Loggers
- Spyware and Adware
- Data Interception – Wired and Wireless
- Spam/Phishing emails
What Are The Key Concerns?

• Any computer connected to another computer
• Computers left unsecured and unattended
• Notebook computers can be lost/stolen
Vulnerability When Connected To A Network

- Internet via Cable modem, DSL or dial-up modem
- Wireless access in cafes, hotels, airports
- Local network
- Direct connection to another computer
What Can Be Done?

• The following 10 tips should be used to protect valuable data for both you and the college
Keep Software Up-To-Date (Windows)

- Run Windows update through Internet Explorer
- Automatic update notification - run Microsoft Updates when notified (lower right hand side corner - yellow shield with exclamation mark)
- Search for available updates using:
  - http://www.windowsupdate.microsoft.com

Tip 1 for protecting data
Keep Software Up-To-Date (Apple)

- Mac OS X & Apple Applications
  - Automatic updates enabled in System Preferences
- Microsoft Office & Adobe applications
  - Automatic update notification
- Enable automatic version checking in other applications when available
- Easy search for available updates using:
  - http://www.versiontracker.com/
  - http://www.macupdate.com/

Tip 1 continued for protecting data
Always Run Anti-Virus Software (Windows)

- Symantec Anti-virus software installed
- Virus definitions are kept up-to-date by via an automatic update while on campus network
- Manual update via Symantec Shield - LIVE UPDATE

Tip 2 for protecting data
Always Run Anti-Virus Software (Apple)

- Symantec Anti-virus software installed
- Virus definitions are kept up-to-date by via a scheduled daily update (@ 12:00pm)
- Hard drives scanned on a regular schedule (user directory every day @ 12:15pm, entire hard drive every Friday @ 12:30pm)
- Use Symantec Scheduler (via menu bar icon) to adjust schedule if not convenient

Tip 2 continued for protecting data
Use Personal Firewall Software and VPN

- (Apple) Firewall built-in to OS X, located in the Sharing pane of System Preferences
  - Already turned on for new Macs and Windows machines on campus

- Minimize open ports
  - (Apple) Ports automatically opened in OS X when services turned on in Sharing pane in System Preferences

Tip 3 for protecting data
Use Strong Passwords

- Password complexity
  - Uppercase, lowercase, numbers & symbols
- Password expiration
  - Passwords expire after 180 days
  - Warning via email 14 days before it expires
  - Only Help Desk can change it after expiration
- Password history
  - Can’t reuse your last 3 passwords
Password Guidelines

• Minimum password length
  • At least 7 characters for any network password

• Never share your password

• Change password after working with a technician or any IS staff who has been in contact with your machine.

• (Apple) Use OS X keychain to store passwords. Make sure to choose a very secure password for your OS X keychain.

Tip 4 continued for protecting data
Beware of Password Phishing

- Information Services will never ask for your password in an email message.
- Emails that ask for your email account password or that warn you that your email account is over quota and provided a link for you to log in to your email account are phishing attempts even if they appear to have been sent by the college’s network services.

Tip 5 for protecting data
Protect Notebook Computers

- Locks, cables and alarms
- Not in checked luggage
- Inconspicuous carrying case
- Don’t leave notebook unattended

Tip 6 for protecting data
Protect Personal Information*

- Confidential data
- Non-public financial information
- Protected health information
- Private educational records
- Usernames and passwords

*"Personal Information" means information capable of being associated with a particular individual through one or more identifiers, including, but not limited to, a Social Security number, a driver’s license number, a state identification card number, an account number, a credit or debit card number, a passport number, an alien registration number or a health insurance identification number, and does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media

Tip 7 for protecting data
Use Encryption

• Both Apple and Windows machines offer built in encryption tools, please contact the Help Desk at ext. 4357 to arrange for assistance in this area

• IS strongly encourages users to use encryption for any sensitive data that must reside on a computer

Tip 8 for protecting data
Back Up Your Data

• Users are responsible for data backups
• (Apple) OS X 10.5 and later includes Time Machine backup software
• (Windows) Users can manually backup data as needed
• Methods of backup include:
  CD, DVD, USB drive, network storage

IS strongly recommends that users DO NOT store confidential data of any kind on their computer.

Tip 9 for protecting data
Beware of copyright laws

• Illegal File Sharing

It’s this simple: it is a federal crime to distribute or download copyrighted music, movies or software on the Internet without permission from the copyright owner. The RIAA (Recording Industry Association of America) continues to search peer-to-peer (P2P) networks such as Limewire, BitTorrent and Ares in its efforts to identify illegal file sharing activity and seek compensation for its clients in the music industry. You are not anonymous when using P2P file sharing sites!

• [http://www.conncoll.edu/Libraries/policies/mediadownloadpolicy.html](http://www.conncoll.edu/Libraries/policies/mediadownloadpolicy.html)
• [http://www.conncoll.edu/Libraries/policies/copyright.html?tm=102055471](http://www.conncoll.edu/Libraries/policies/copyright.html?tm=102055471)

“Members of the campus community are advised to become as knowledgeable as possible regarding copyright and fair use as it pertains to their discipline. Connecticut College does not accept legal responsibility for copyright infringement by individual members of the College community. Individuals who willfully disregard College policy and guidelines do so at their own risk and assume all liability.”

Tip 10 for protecting data
Overview of What Can Be Done

- Keep software up-to-date
- Always run antivirus software
- Use personal firewall software
- Use strong passwords
- Beware of Phishing attempts
- Protect notebooks when traveling
- Protect Personal/Confidential Data
- Encrypt sensitive files and folders
- Back up your data files
- Follow and be aware of Copyright laws

Top 10 Tips to remember for Protecting Your Data
Other things you should do to secure Your Computer

• Require a password to log in, wake from sleep or wake from screen saver

• Put computer to sleep or “lock” the computer when walking away
Use care with Email and Instant Messaging

- Never send sensitive information without encryption
- Be very cautious before clicking on links
- Check configuration settings for unnecessary or unsecure “features”
- Turn off file sharing features
Web Browsing and Software Downloading

• Keep your web browser up-to-date
  • Safari, Firefox and Chrome web browsers all use Google’s malware database to alert you to bad sites and support Extended Validation (EV) Certificates

• Campus Macs are configured to handle all common video formats
  • No need for Windows Media Player or extra codecs

• Only download files from trusted sources
• Watch installations for “optional” applications
• Pay attention to requests for your to enter your administrator password
Questions?

• Contact the Help Desk
  • Basement of Shain Library
  • x4357
  • help@conncoll.edu
  • AIM: camelcomphelp
Send Us Your Feedback

• Email
  • mcdre@conncoll.edu (Apple)
  • kjdim@conncoll.edu (Windows)

• Send an anonymous note to:
  • Attn: Kevin DiMinno or Mike Dreimiller - Hamilton Basement
This has been a presentation of Information Services