



Top Five Computer Tips for St. Kate's Students

WIRELESS NETWORK ACCESS TO ST. KATE'S SYSTEMS REQUIRES SETTING UP AN ENCRYPTED NETWORK CONNECTION:

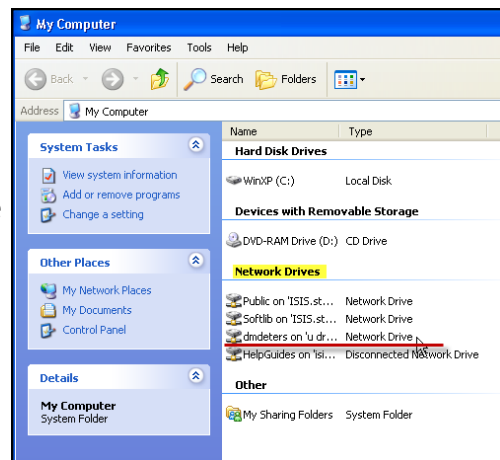
- We have 'How To' Help Guides on our website, at <http://www.stkate.edu/mcglynn>. There are instructions for Windows XP, Windows Vista and Mac OS X 10.3, 10.4, 10.5 Search for Wireless to find the right document to setup your computer or bring it to the Help Desk.
- The CSC-student network profile must be added to any computer that needs access to secure systems such as web-mail or KateWay.

FREE ANTI-VIRUS SOFTWARE IS AVAILABLE TO ALL STUDENTS:

- Residence Hall students are required to install our McAfee Enterprise Anti-Virus software. Commuting students are welcome to stop by the Help Desk for a free copy. Make sure you uninstall any other anti-virus software on the computer before installing McAfee.

ALL STUDENTS HAVE A NETWORK DRIVE FOR SAVING FILES:

- Each student receives a 'U' drive on the network. If you open My Computer or Windows Explorer on a Lab PC you will see the 'U' Drive along with the 'P' drive where the College community store shared files.
- SPECIAL NOTE TO LAB USERS: Do not save files on the C drive or Desktop of Lab PCs. User login profiles are deleted daily. Files saved to the local drive will be lost. Use the U drive or a flash drive to save your work. Also note, U drives cannot be accessed from off campus. E-mail a copy of the file to yourself if you are working on it off campus.



DON'T EDIT E-MAIL ATTACHMENTS INSIDE OF WEB-MAIL:

- Choose the option to save the attachment then browse to it to open with My Computer or Windows Explorer. Editing files in web-mail means you are editing a temporary file in a hidden folder on the computer. If you choose to edit in web-mail you must select save-as, and store the file on a network or flash drive. **If you don't, all your work will be lost.**



SPYWARE AND VIRUSES LURK EVERYWHERE ON THE WEB:

- The Help Desk sees a hundred or more PCs infected each term. Instant Messaging and social networking sites are frequently targeted with identity theft scams or malicious spyware. Music sharing software such as Limewire and Kazaa are common targets as well. Instant message attachments are often used to transmit Trojans and viruses.
 - Scan for viruses at least weekly and install one of the legitimate anti-spyware programs. Go to www.download.com, to select a software tool. We recommend Malwarebytes and Spybot Search & Destroy. The software is free, a donation is recommended.
 - Practice Safe Computing! Learn more about protecting your computer!
- ⇒ View [documents discussing how to keep your computer as safe as possible.](#)