Good Computing Practices for General Users

1. Use strong passwords that can't be easily guessed, and protect your passwords.
   - Don't share your passwords and avoid writing them down.
   - Characteristics of good, cryptic passwords:
     - At least 8 characters in length
     - Contain a mixture of upper and lower case letters, numbers, and symbols
     - Difficult to guess (e.g. don't include real words or personal information like user name, names of family members, places, pets, birthdays, addresses, hobbies, etc.)
     - Easy to remember (so you don't have to write them down)
2. Be cautious when using the Internet.
   - Don't provide personal or sensitive information to Internet sites, surveys or forms unless you are using a trusted, secure web page.
   - Also, just opening a malicious web page can infect a poorly protected computer. Be aware of where you are going before clicking on a web link. When in doubt, instead of clicking on an unknown or unsolicited link, look up the web site on your own and go there independently.
   - Be extremely careful with illicit file sharing software. Violators risk being disconnected from campus networks. If you share copyrighted files, you also run the risk of serious legal consequences.
3. Practice Safe Emailing.
   - Don't open email attachments or click on web site addresses in emails unless you really know what you're opening.
   - Delete spam and suspicious emails; don't open, forward or reply to them.
4. Secure your area before leaving it unattended.
   - Lock windows and doors.
   - If you are an employee, be sure to lock up portable equipment and sensitive material before you leave your work area (take keys out of drawers), and never share your access code, card or key.
5. Secure laptop computers at all times: keep it with you or lock it up securely before you step away.
   - At all times: in your office or dorm room, at coffee shops, meetings, conferences, etc. - Remember: laptops get stolen from cars, houses, and offices all the time.
   - Make sure it is locked to or in something permanent.
6. Shut down, lock, log off of, or put your computer to sleep before leaving it unattended, and make sure it requires a password to start up or wake-up.
   - <ctrl> <alt> <delete> or <Windows><L> on a PC;
   - Apple menu or power button on a Mac;
   - Talk to your computer support for assistance if it doesn't.
7. Make sure your computer is protected with anti-virus and all necessary security "patches" and updates, and that you know what you need to do, if anything, to keep them current.
   - Talk to your computer support person for assistance.
8. Don't keep sensitive information or your only copy of critical data, projects, files, etc. on portable devices (such as laptop computers, CDs/floppy disks, memory sticks, PDAs, data phones, etc.) unless they are properly protected. These items are extra vulnerable to theft or loss.
9. Secure files with confidential or sensitive information (including social security numbers and birthday) with encryption and ensure they are encrypted whenever you leave them unattended.
   - Talk to your computer support person for assistance.
10. Don't install unknown or unsolicited programs on your computer.
    - These can harbor behind-the-scenes computer viruses or open a "back door" giving others access to your computer without your knowledge.
11. Make backup copies of files or data you are not willing to lose -- and store the copies very securely.