UNCG ITS Top 10 Safe Computing Practices

As a UNCG employee, you are responsible for maintaining the integrity and security of University information and computing resources. The following ten tips will help you meet this expectation.

1. **Use strong passwords and keep them secure.** Good passwords use a combination of mixed-case letters, numbers and symbols. They should be easy for you to remember and hard for others to guess. Never share your credentials. For password creation tips, visit *http://its.uncg.edu/Accounts/Tips*.
2. **Protect your workstation with a firewall and anti-virus software.** Most University workstations are directly accessible from the Internet and must be protected from attack. Modern operating systems have an integrated firewall—make sure it is turned on and properly configured. To protect your system from malicious software use anti-virus software and keep your virus definitions up-to-date. Using ITS-provided software images provide both anti-virus and firewall protection.
3. **Keep workstations patched and up to date.** An out-of-date operating system or application can make it easy for an attacker to exploit your computer. ITS-provided software loads will update the operating system automatically. You are responsible for updating the additional software you may use.
4. **Use email responsibly.** Be wary of suspicious attachments. Be cautious of embedded links; type them into your web browser instead of clicking to ensure you reach the site you plan on reaching. Do not forward or reply to spam or suspicious emails. Do not use email to transmit unencrypted restricted data.
5. **Lock, log out of, or shut down your workstation when not in use.** When leaving your computer unattended, lock the computer or log out of your user account to prevent unauthorized use.
6. **Store restricted data on University servers.** Saving data to your local hard drive, printing it or transferring it to a PDA or laptop can increase the risk to that data. Unless there is a clear business need and proper precautions are in place, restricted data should reside only on University-managed servers.
7. **Do not install unnecessary software.** Some software contains malicious code that allows the provider to access your computer or track your activity. Other software may be innocuous in itself but offer an attacker new ways to compromise your computer. A safe strategy is to only install the software required to perform your duties from ITS-managed sources.
8. **Back up your data.** In addition to avoiding a loss of work, University data must be preserved for the purposes of records retention policy and compliance. If you work with restricted data, backups should be subject to the same protections as the active data.
9. **Securely destroy media when it reaches end-of-life.** Before disposing or transferring a computer, media or other data storage device, ensure that the storage medium has been securely wiped to prevent data exposure.
10. **Physically secure the equipment in your care.** Lock your office when you are away. Keep media, laptops and other mobile computing devices locked up when unattended.

For assistance with these items or for additional computing help, please contact the ITS Service Desk at **256-TECH (8324)** or at **6tech@uncg.edu**.