Technology Tips

1. Data on paper is the same as data on the screen. When you print sensitive/confidential information it is important that you shred it when your are finished reviewing it. ALL units should have a shredder.

2. Access to University data is provided to University employees for the conduct of University business only. Faculty must follow data privacy laws (FERPA).

3. Back up any data that is not stored in your home drive (My Documents folder) regularly.

4. Log-off your computer at the end of your work day, this allows your computer to accept the updates sent by ITS.

5. Pay attention to ITS Campus Alerts, they will keep you up to date on the latest security issues affecting our network.

6. Save files often while working.

7. Know NCCU Policies and Procedures regarding Information Technology.

8. Call the Eagle Technical Assistance Center (ETAC) at 530-7676, for assistance.

Please Ensure You Adhere To The Warning You See Before You Log-Into Your Computer

This is a North Carolina Central University computer system and may be used by, authorized personnel only. Use of this system by any user constitutes consent to, university IT policies and federal, state, and local laws. Unauthorized use of this, system by any user may result in criminal, civil, and/or administrative penalties., This system is provided for the purpose of facilitating the business of the university, including teaching, learning, scholarship, research, communication, and other, creative endeavors. In providing and maintaining its electronic communication, infrastructure, the university complies with applicable federal, state, and local laws, and it requires that all users do the same. Violations of the law may be reported to, the appropriate civic authorities. Violations of university policy and standards will, be processed through the responsible university authorities. Access to computing, resources may be restricted or denied, without warning, as a result of violations of, law or university policy.

Information Technology Services
North Carolina Central University
(919) 530-7676 | HELPDESK@NCCU.EDU

Information Security Awareness

North Carolina Central University
Information Technology Services

As an institution of higher learning, North Carolina Central University encourages, supports, protects, and embraces freedom of expression to pursue scholarly inquiry and to share information with the global academic community.

To maintain a secure and reliable network, NCCU Information Technology strives to inform all NCCU employees and students of the policies, which govern the use of NCCU computing services and networks.

This brochure is designed with students in mind. In it you will find information on where to find policies and tips on how to secure your computer.

We use computers for many important parts of our lives. There are many programs out there that can hack into your system. Protect your computer with:

Antivirus software
Anti-Spyware Software
Update Windows
Firewalls
Back-up system
Password protection

Desktop Security

1. ALWAYS lock your computer when you are walk away.
2. Passwords should not be written on "sticky notes" place on your computer or other locations within your office.
    a. Passwords should not be your first initial, last name.
    b. Password should be a minimum of 8 characters.
    c. Passwords should be changed minimum every 90 days
    d. Do not share passwords with co-workers or students.
3. Store all your documents on your NCCU home drive (My Documents folder). This information is stored on the network server and backed up daily.

E-Mail Security

1. Your NCCU e-mail is the "official" university provided e-mail address and all work related correspondense should be sent from/to this address. An alternate email address must be submitt frist sign-on to your NCCU e-mail.
2. Don't open SPAM e-mail, just Right-Click on them and select Delete.
3. NEVER respond to SPAM messages.
4. Be aware that by adding your name to listservs and other distribution list, outside the university- you are setting yourself up for SPAM e-mail. **Vendors sell their distribution lists.**
5. ITS will NEVER ask for any personal information (userID, password, etc.) via e-mail. Watch out for e-mails that appear to come from campus accounts asking for personal information.
6. Forward instances of spam/phishing e-mails to: spam@nccu.edu
7. Keep your e-mail healthy by keeping your inbox small.
    a. Often e-mail is slow because your inbox is too large, making loading times of your inbox slow.
    b. If your inbox becomes too large (greater than 500 MB), it may become corrupted and your could lose e-mails or miss incoming messages.
8. Don't send sensitive files as e-mail attachments unless they are protected.
9. Remember that e-mail is not always secure, don't send any information that you do not want on a billboard.
10. E-mail account passwords must be changed at least once every 90 days.

Banner Security

1. NEVER share Banner Passwords or Banner Account Information.
2. ALWAYS follow Banner Data Standards if you input data into Banner.
3. ALWAYS alert ITS when an employee leaves the university or have a change in job duties.
4. NEVER allow anyone to perform work in your account.

Internet Security

The Internet is a vast resource of knowledge; however, it is also filled with dangers. Some dangers can be avoided by using common sense.

Websites such as Facebook.com and MySpace.com can be fun ways to express yourself; however, setting up profiles which contain personal information such as home address, phone number, or birthday should be avoided as well as posting information or images which could be damaging to NCCU account or to you.

Don't become a victim—keep your personal information off the internet. Information such as your full name, home address, phone number, Social Security Number, passwords, names of family members, and account information such as bank and credit card numbers, should not be posted on the Internet or shared with online friends.

Surfing without protection and common sense increases the odds that your system or personal information could be compromised.