ITS provides the following services:

- Network troubleshooting
- Exam scanning and classroom support for instructors
- Software and hardware troubleshooting and resolution
- Computer repair (CRC) for CCI computers
- Account management
- Software distribution and updates
- Residential computing services (ResNET)

As part of the university’s coordinated technology plan, the Carolina Computing Initiative (CCI) aims to ensure that Carolina students, faculty, and staff have easy access to high-quality and affordable technology and can use it effectively.

ITS technical support is available to the UNC-CH computing community 24 hours a day 365 days a year. You can submit Help Requests to the IT Response Center using any of the following options:

- Go to http://its.unc.edu/itrc and click on the "Submit a Help Request" link
- Call (919) 962-HELP
- Chat Online with the Help Desk at help.unc.edu/chat
- Visit the ITRC in the Undergrad Library or Student and Academic Services Building.

The ITS Response Center (ITRC) provides walk-in support at two locations:

In the basement of the
R.B. House Undergraduate Library
(next to the Pit)

Student and Academic Services Building
(South Campus)

For more information about identity theft, see:

- Department of Justice: www.usdoj.gov/criminal/fraud/idtheft.html
- Federal Trade Commission: www.ftc.gov/bcp/edu/microsites/idtheft
- Social Security Administration: www.ssa.gov/pubs/idtheft.htm
- ID Theft Survival Kit: www.identitytheft.org
- NoScamNC
  http://noscamnc.gov
- AnnualCreditReport.com’s FAQs page: www.annualcreditreport.com/cra/helpfaq
- HelpSite’s Basic Security Checklist:
  http://help.unc.edu/?id=1629
- Campus Security Services:
  www.unc.edu/security/campus

Hours:

**Monday-Thursday**
7:30AM - 10:00PM

**Friday**
7:30AM - 5:00PM

**Sunday**
1:00PM - 10:00PM
PASSWORD PROTECTION

5 reasons to change your password
every 30 days:
1. Frequently changing your password increases the degree of randomness.
2. A personal password helps protect your account from being accessed by others.
3. You will not be able to publish web pages or use other digital services until your password has been updated.
4. Accounts with temporary passwords may be deactivated.
5. The longer you wait before changing passwords, the more difficult it will be to get used to the new one.

How to create a secure password:
- The best solution to password security is to not give out your password at all. Allowing someone else to have access to your password could affect your system protection. Make your password 8 characters long. The longer it is, the more difficult it will be to discover with a brute force search.
- Use as many different characters as possible when forming your password. Include at least three of the following: uppercase letters, lowercase letters, numbers, special characters, spaces, e.g. L8ght97, ST@rs99.
- Passwords should be easy to remember, so they do not have to be written down.
- You should be able to type your password quickly so no one can look over your shoulder and see it.

Methods of password cracking:
Crackers commonly use two main approaches to obtain passwords.

- The BRUTE FORCE method. This method works by trying out every possible combination of characters to find the correct password. Cracking times with this method vary from a few seconds to thousands of years depending on the length of the password and the number of different character types used. This is why it is important to use long passwords with a variety of different characters.
- The DICTIONARY method. These programs use long lists of commonly used words from various languages, including names and words not appearing in dictionaries, such as places and film titles. They also test a number of variations of the words including backwards, substituting numbers for letters, and capital and lowercase combinations.

Don’t make it easy!
Because of the prevalence of cracking software, you should not use any information that is commonly targeted by these programs.

- Do not use personal information or information that is easily obtained about you, e.g. any name, phone number, Social Security Number (SSN), license plate number, birth date, address, etc.
- Do not use names of acquaintances
- Do not use anybody’s birth date
- Do not use words, geographical names or biographical names that are listed in standard English or foreign dictionaries.
- Do not use a place or a proper noun
- Do not use any of the above spelled backwards and/or followed by or preceded by numbers
- Do not use passwords that are easy to spot while you’re typing them in, like 12345, qwerty (all keys right next to each other), or nnnnnn
- Do not use any previous password you have used
- Do not use part or all of your User ID

IDENTITY THEFT PROTECTION

Identity theft occurs when someone uses your name, address, Social Security Number (SSN), bank or credit card account number, or other identifying information without your knowledge to commit fraud or other crimes.

Protecting against identity theft:
- To order a free copy of your credit report, go to: www.annualcreditreport.com
- Place passwords on your credit card, bank and phone accounts.
- Don’t give out personal information over the phone, through the mail, or over the Internet unless you’ve initiated the contact or are sure you know who you’re dealing with.
- Guard your mail and trash from theft.
- Before revealing any personal identifying information, find out how it will be used and secured, and whether it will be shared with others.
- Ask if you have a choice about the use of your information.
- Don’t carry your Social Security card; leave it in a safe place.
- Give your SSN only when absolutely necessary.
- Pay attention to billing cycles. If you don’t receive your bills on time, follow up with the creditor. A missing credit card bill could mean an identity thief has taken over your account and changed your billing address to cover his tracks.
- Be wary of promotional scams.

Steps to take if YOU are a victim of identity theft
1. Contact the fraud department of one of the three major credit bureaus. As soon as that agency processes your fraud alert, it will notify the other two, which then also must place fraud alerts in your file:
   - Equifax: www.equifax.com
   - Experian: www.experian.com
   - TransUnion: www.transunion.com
2. Close the accounts that you know or believe have been tampered with or opened fraudulently.
3. For check fraud, contact the three major check verification companies:
   - TeleCheck - 1-800-710-9898
   - Certezy, Inc - 1-800-437-5120
   - International Check Services - 1-800-631-9656
4. File a police report.
5. File a complaint with the Federal Trade Commission by going to:
   www.ftc.gov/credit