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 ITS Response Center using any of the following options:
- Go to [http://its.unc.edu/itrc](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)

**Hours:**
- Monday-Thursday 7:30AM - 10:00PM
- Friday 7:30AM - 5:00PM
- Sunday 1:00PM - 10:00PM

**Student and Academic Services Building**

(South Campus)

**Hours:**
- Monday-Thursday 7:30AM - 10:00PM
- Friday 7:30AM - 5:00PM
- Sunday 1:00PM - 10:00PM
EMAIL PROTECTION

Summary
Currently, the most effective method of virus delivery is through the use of email attachments. Virus writers use clever and mysterious subject lines and messages to pique the curiosity of users, causing them to open the attached virus file. Approaching each email attachment with suspicion and caution can save headaches, time, and money by avoiding virus infection and its consequences.

Email Attachment Security Tips
- Never enable JavaScript for email or email attachments.
- Never use email to send confidential information such as credit card numbers, bank account numbers, or your Social Security number.
- Never respond to email asking for confidential information.
- Never allow an executable email attachment to launch on its own.
- Never allow your email client to “View Attachment Inline.”
- Never open email attachments from strangers.
- Disable HTML for email.
- Disable cookies for email.
- Use a virus scanner.

Before Opening Attachments
You should apply the following five tests to every piece of email with an attachment that you receive. If any test fails, delete that email. If they all pass, then you still need to watch for unexpected results as you read the message.
1) The Know test: Is the email from someone you know?
2) The Received test: Have you received email from this sender before?
3) The Expect test: Were you expecting email with an attachment from this sender?
4) The Sense test: Does email from the sender with the contents described in the Subject line and the name of the attachment(s) make sense? For example, would you expect the sender — let’s say your Mother — send you an email message with the Subject line “Here you have, :)” that contains a message with attachment “AnnaKournikova.jpg.vbs”? A message like that probably doesn’t make sense, but it happens to be an instance of the Anna Kournikova worm, and reading it can damage your system.
5) The Virus test: Does this email contain a virus? To determine this, you need to install and use an anti-virus program.

SPAM — the definition
Spam is the word used to describe unwanted email. The term is most often associated with Unsolicited Commercial Email also commonly known as UCE, but it also applies to any other type of undesirable or unwanted commercial traffic such as commercial Usenet postings, instant messages promoting websites, and other such items.

SPAM Reduction Tips
- When you receive a UCE, delete it. Never click on any web links or open attachments associated with UCE.
- When you receive a UCE, do not reply. If you are given the option to remove your address, do not do so unless you are certain the organization is reputable. This is usually just a way for the originator to verify that your address is still actively used. If you request to be removed from the list, your address may simply be resold to another UCE distributor.
- Avoid giving out your primary email address. Guard your main email address just as you would your telephone number. Your main email address is what you would give to friends, family, and business associates. Unless there is a specific reason to give out your main email address to someone other than those you know, consider using a second email address when filling out forms that might potentially lead to your address being sold or leased to other companies, or else use a fictitious email address when completing such forms online.
- Do not publish your email address on a webpage on the open internet. Many automated computer programs “harvest” email addresses from webpages and add them to mailing lists which they then resell. You can disguise your email address by stating it in words, so that the address Leon57@email.com could be presented on the webpage as “Leon57 AT email DOT com.”
- Do not use an email alias based on a simple name. Many automated computer programs mail by brute force, sending emails to albert@email.com, amy@email.com, and so on, testing to see if each name is a possible email address. If you use an email alias that cannot be automatically generated by a machine you are less likely to receive unsolicited email.
- Never buy anything advertised in unsolicited email. Marketers use this technique because it is effective. Companies pay bulk emailers to distribute this unsolicited email; they will not continue to spend money on bulk email unless it is effective.
- Use an email program to block UCE. This makes it easier to filter unwanted email. A good program to use can be downloaded for free at http://spambayes.sourceforge.net

More Information
For more information about reducing SPAM, visit the HelpSite article at http://help.unc.edu/?id=5761.