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](http://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)

<table>
<thead>
<tr>
<th>Hours:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monday-Thursday</td>
</tr>
<tr>
<td>7:30AM - 10:00PM</td>
</tr>
<tr>
<td>Friday</td>
</tr>
<tr>
<td>7:30AM - 5:00PM</td>
</tr>
<tr>
<td>Sunday</td>
</tr>
<tr>
<td>1:00PM - 10:00PM</td>
</tr>
</tbody>
</table>

---

**Student and Academic Services Building**
(South Campus)

<table>
<thead>
<tr>
<th>Hours:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monday-Thursday</td>
</tr>
<tr>
<td>7:30AM - 10:00PM</td>
</tr>
<tr>
<td>Friday</td>
</tr>
<tr>
<td>7:30AM - 5:00PM</td>
</tr>
<tr>
<td>Sunday</td>
</tr>
<tr>
<td>1:00PM - 10:00PM</td>
</tr>
</tbody>
</table>

---

For more information on **System Hardening**, use the following resources:

- The HelpSite has an article on suggested best practices for securing Windows which can be found at [http://help.unc.edu/2512](http://help.unc.edu/2512)
- Suggested best practices for Novell are located at [http://help.unc.edu/3923](http://help.unc.edu/3923)
- There is also an article on securing your computer on the UNC network at [http://help.unc.edu/1290](http://help.unc.edu/1290)
Workstation and System Security

The Department of Homeland Security (DHS), EduCause, National Security Agency (NSA), National Institute of Standards and Technology (NIST), and many others publish guides to help protect computers and information. Internet Security Alliance (ISA) in collaboration with DHS has developed a Common Sense Guide to Cyber Security that has twelve specific recommendations that the Information Technology Security Office suggests anyone to follow for their protection of personal computers and information.

Many attacks on Internet and network systems have no particular target. The attacker simply sends a large broadcast that uses any unprotected system as a staging point from which to launch an attack. Using computers without basic protections like user education, firewalls, and antivirus software not only affects your own system, but many other systems as the virus is spread around the Internet.

Your system’s lack of protection can make you a target, destroying your computer, your network, and contributing to a virus distribution that slows or halts portions of the Internet. All of us who use the Internet have a responsibility to help create a culture of security that will enhance consumer and business confidence. More importantly, failing to heed best practice advice could hurt you personally and significantly.

10 STEPS for Workstation and System Security

Use strong passwords and change them regularly
A password should not be easily guessed. Do not use dictionary words from any language, names, or minor variations of these. Consider using a combination of letters, both upper and lowercase, numbers, and punctuation marks. Lengths can vary (a minimum of 8 characters; longer is better). Construct the password using a pattern so that you can remember it whenever you need it without having to write it down to jog your memory. You should always change default passwords and initial access passwords set by someone else as soon as possible.

Look out for e-mail attachments and internet download modules
- Do not use the “preview” function for e-mail contents.
- Do not open an attachment that the antivirus software has indicated is malicious.
- Do not open e-mails from someone you do not know — delete them instead.
- If you know the sender or decide to open the e-mail, check to make sure the contents along with the names of attachments and the subject line make sense.

Install, maintain, and apply antivirus programs
Install University approved antivirus software on every machine and keep the signature (dat) files current through automatic or manual updates at least once per day. Do not connect to the Internet without first activating an AV program. Schedule an AV scan or examination of all files on a regular basis, preferably weekly, to catch problems missed at other checkpoints.

Install and use a firewall
Install firewall software on every machine and set it up to block traffic for all service except those specifically used on the machine. While the firewall rules are being crafted, there will be instances of over-blocking, making the use of some computer service more difficult.

Remove unused software and user accounts
Clean out everything on an equipment that has been replaced. Remove accounts that are no long used or necessary. Disable or remove any unneeded software, programs or services (i.e. games, free download software, music players, etc.).

Create backups for important files, folders, and software
Backup all files on an established schedule. To select appropriate frequency for backups, remember that changes to the original between the time of backup creation and loss would have to be applied manually. Retain backups over a period of time to allow for fixing a problem that is not discovered right away. Special backups such as calendar year-end should be saved for several years. Periodically test the backup process by restoring the content to an alternate location and checking it for accuracy.

Keep current with software updates
When you purchase a program, see if and how the vendor supplies updates. Learn how the vendor provides answers to questions about problems with their products.

Consider purchasing extended warranty support if it is available. If patches are not supplied, find out when new releases are available and consider upgrading if vulnerability fixes are included. Locate and apply vendor software updates, especially patches for known vulnerabilities, as soon as possible. Consult the vendor’s website to see how to get timely e-mail notices about patches. Subscribe to a vendor mailing list for notification of problems and fixes.

Implement network security with access control
Access to each component on the network should be limited to protect it from improper access and harm. Basic access protection can be implemented using strong passwords. Turn off the file and printer sharing feature on each computer unless it is in use, particularly when accessing the Internet using cable modems, digital subscriber line (DSL), or other high-speed connections. Do not select the option on web browsers for storing or retaining user names and passwords. Require authentication for wireless and remote access.

Limit access to sensitive and confidential data
Take extra caution not to share sensitive and confidential information electronically. Do not use real information for any testing of new processes. Do not use public or Internet café computers to access online financial services accounts or perform financial transactions. Do not disclose personal, financial, or credit card information to a little-known or suspect website.

Get technical expertise and outside help when you need it
Ask the organization handling your technology support how they are addressing security practices and if they need additional assistance.