ITS Support of University Emergency Notification Solutions

**Campus Improves Ability to Reach Students, Faculty, and Staff in a Crisis**

Over the past year, ITS representatives have been part of a campus-wide team charged with improving the University’s emergency notification and communication tools. ITS partnered with campus entities and outside vendors to develop technology solutions in support of this effort. These solutions include:

- **Cell Phone Notification - Management**

  Information Systems wrote an application in UNCGenie that gathers cell phone numbers, allowing students, faculty, and staff who provide such contact information to receive emergency text or telephone message notifications. UNCGenie users are prompted to update their contact information at regular intervals.

- **Alert Pop-Up Messages - Windows**

  based computers connected to the Internet are now able to receive alert “pop-up” messages if the proper notification software—a program written by Application Services—has been installed. To access this software, go to [http://uncg-campus.info/go/page/1365/25335/](http://uncg-campus.info/go/page/1365/25335/). All new computers that receive the ITS standard software load will have this application installed.

- **Emergency Streaming Radio - Application Services and Network Operating Systems**

  collaborated on an online emergency notification tool that provides 24 x 7 streaming from UNCG’s Information Radio Station (1640 AM). To access the radio stream through your default media player, visit the emergency information Web site at [http://www.uncg-campus.info](http://www.uncg-campus.info) and click on the “Listen in your media player” link.

- **Blue Light Telephone Tower Broadcasting, Sirens - Sixteen “blue light” emergency telephone towers on campus are equipped to broadcast messages and to sound sirens. UNCG Police is able to transmit broadcasts either remotely or at the tower location. Telephone Services installed the broadcasting devices, which operate over the campus network. UNCG plans to conduct a comprehensive test of these emergency notification and communication tools this fall. For more information about these tools and others, visit [http://www.uncg-campus.info](http://www.uncg-campus.info).**

UNCG to Co-Host Information Technology Conference

**System-wide Opportunity to Exchange Ideas and Information**

The University of North Carolina College and University System Exchange (UNC CAUSE) conference is an opportunity for technologists from all areas of the UNC system to exchange information. UNCG will co-host UNC CAUSE in downtown Greensboro from November 17-19.

The theme for this year’s UNC CAUSE conference is “The University of North Carolina Tomorrow: Striving for Excellence Through Technology and Collaboration.” UNC CAUSE itself has been an ongoing collaboration between UNC faculty and staff since 1974. Around 325 UNC staff plus up to 75 vendor representatives are expected to attend this year.

UNC CAUSE features presentations by both vendors and staff from the UNC system. The UNC CAUSE planning committee received a great response from the call for presentation proposals. UNC staff will deliver presentations on topics ranging from enterprise administrative systems to academic support. ITS staff will be involved in nine presentations at the conference. Vendor presentations are tailored to challenges that are common in university environments. UNC CAUSE also includes informal “Birds of a Feather” sessions, which are opportunities for people interested in a given topic to exchange ideas and experiences.

For more information about this year’s UNC CAUSE, visit [http://www.uncg.edu/cause08/](http://www.uncg.edu/cause08/).
Wireless Network Expansion and Security

ITS continues to expand wireless coverage and security this fall. The areas now targeted for expansion are frequently-used outdoor areas such as the Brown courtyard, the lawn in front of the Elliott University Center, the seating areas and entry gates of the athletic stadiums, and the courtyard between the Stone, Forney, and McIver Buildings.

This expansion involves the installation of an additional twenty wireless access points and should be complete by the end of November. ITS will also be installing monitoring devices that prevent unauthorized wireless access points from joining the UNCG network and creating a possible security risk. These monitors will be in place by mid-November.

If you have any questions about wireless network expansion or security, contact Natsu Carr, ITS Project Manager, at 334-4160.

Campus Technology Updates

Faculty/Staff Email Project

ITS is currently engaged in an ongoing project to evaluate the viability of outsourcing faculty and staff email. Earlier this year, UNCG decided to outsource student email to Google through its Google Apps for Education (GAFE) program. iSpartan is UNCG’s implementation of the GAFE program. Although faculty and staff may log in to and access certain features of iSpartan, such as Docs, Sites, and Talk, email for faculty and staff is still being delivered via e-Spartan (UNCG’s implementation of Lotus Notes). Go to http://its.uncg.edu/Projects/Apps_for_Education for more information about iSpartan.

Student Laptop Initiative

ITS and the Academic Technology Coordinating Committee have chosen the new Lenovo ThinkPad models for the Student Laptop Initiative (SLI). The new models are lighter, have a faster processor, longer battery life, and a built-in camera. The new MacBook offerings have not been finalized. ITS expects the new models (Lenovo and MacBook) will be available for purchase by mid-November. For more information as it becomes available, visit the SLI Web site at http://its.uncg.edu/Laptop/.

Deadlines: ITS Computer Lab Reservations and Software Requests

- October 31
  Submit requests to reserve ITS computer labs for the spring semester. This deadline refers to the submission of departmentally-coordinated reservations. These requests for lab space should be coordinated first at the departmental level or by lab committees before sending them to ITS. After this deadline, faculty requests will be handled on a first-come, first-served basis. Information about the reservation process, including the Lab Reservation Request Form, can be found at http://its.uncg.edu/Labs/Reservations/.

- November 25
  Submit requests for software to be included in the Spring 2009 ITS PC Computer Lab software load (image). See the guidelines for "Requesting Software for Campus Access" at http://its.uncg.edu/Software/. Before submitting your software installation request, be sure that any "clickwraps" associated with your software request have been approved by the Office of University Counsel. Visit http://www.uncg.edu/ucn/clickwraps/ for more details.

Information Security: Locating Sensitive Data

One of the first steps in protecting a computer system is to understand what information is at risk. The computer itself is a valuable asset to both the University (that paid for it) and computer criminals (who want to use it to send spam or attack other computers), but it is the electronic data that is the greatest potential threat to the interests of the University.

What sort of data and how much of it is on a computer, is often hard to discover. Computers may be shared among different users. A computer may be inherited with a new position. If you visit a Web site containing sensitive data, that data might have been stored on your hard drive.

While there is no magic bullet for finding all types of restricted data, a large percentage of it will be associated with numbers of a specific format: Social Security numbers (identity data), and credit card numbers (financial data). If you could search your computer for these types of numbers, you would be well on your way to locating areas on your hard drive that contain restricted data.

Fortunately, there are tools available to do just this. A word of caution — no tool is perfect. All these tools can do is attempt to locate numbers that seem to match a certain pattern. These tools may not find numbers stored in files using certain proprietary file formats. However, running one of these tools on a regular basis is certainly a business practice that demonstrates a commitment to protecting University restricted data. Instructions for installing and using these tools can be found on the associated Web site.

Cornell Spider for Windows (Mac and Linux are in beta) — http://www.cit.cornell.edu/security/tools/

University of Texas SENF (requires Java, but runs on all platforms) — https://source.its.utexas.edu/groups/its-iso/projects/senf/wiki/SenfVersions

— ITS Security Office