ITS eNews
R·I·T
Information & Technology Services at the Rochester Institute of Technology

Partnering on the RIT Computer Network

By Donna Cullen, RIT Digital Millennium Copyright Agent, Donna.Cullen@rit.edu

Freedom is associated with a mix of rights and responsibilities. At RIT, we seek a balance between academic and personal freedom when using the RIT network and maintaining a secure, fast, and efficient network.

Rather than a destination, the balance is a journey that has seen components come and go. Along the journey, ITS partners with students, systems administrators, faculty, staff and vendors to accomplish our ends. Policy is in place to guide your use of RIT computer and network resources. RIT has put in place some security measures, negotiated reduced prices on software, and reviewed software in order to recommend low cost, compatible options.

RIT Policy
An Acceptable Use Policy (AUP) is associated with the use of any Internet Service Provider (ISP). At RIT, the AUP is called the RIT Code of Conduct for Computer and Network Use. The "Code of Conduct" outlines your rights on the RIT network as well as your responsibilities when using RIT network services.

The RIT Information Security Office (ISO) on campus has issued a host of policies for the protection of information and computer resources on campus. These include requirements for protecting confidential information and for installing and updating software that protects your machine from compromise.

RIT partners with you through policy by giving all community members guidelines for acceptable use and by establishing standards of compliance with basic security measures.

System Wide Initiatives
RIT is seeing success in blocking SPAM before it reaches your inbox. Recent statistics indicate RIT's mySPAM initiative is blocking 90% of incoming SPAM. You receive a daily message indicating which messages were blocked for you. You have the option of reviewing or releasing blocked messages. You also have the option of blocking or allowing all messages from a specific source. Reporting messages that "should" be blocked is easy. Send the message with its full header to spam@rit.edu.

RIT has a firewall in place to protect the central computer resources and information. This limits campus exposure to some exploits. RIT quarantines machines on the network that are known to

be compromised or open to known exploits. Machines are not allowed to register on the network until the machine operating system is patched.

A team of RIT professionals monitor patch announcements and other technical resources to update you and the RIT protection mechanisms. The team – and that includes you – is quite effective in protecting the resources. Exploits are developed rapidly. System and network protection is a journey that means updating operating systems and protection software on a regular basis – *each member of the RIT community is required to comply with this expectation.*

Software acquisition and recommendations
Virus protection software is available free for all RIT students, faculty and staff. Firewall software is available for RIT-owned Windows machines. Current offerings and considerations are available at http://www.rit.edu/its/services/security/ for the entire campus with additional information available for students living in RIT residences available at http://resnet.rit.edu.

Keep in mind, you are required to protect your machine and keep protection mechanisms up-to-date. RIT offers e-Policy Orchestrator for RIT-owned Windows systems as an automated method to ease this task.

Macintosh systems are supported on campus. Virus protection software is available. Exploits for Macintosh systems are limited. Macintoshes running OS X are impacted by some UNIX compromises. Macintoshes running a Windows OS in any configuration are susceptible to exploits of the Windows OS.

Being a Partner
A number of professionals at RIT work with you and for you to protect the RIT network and the machines connected to it. Success in providing the balance of academic freedom and security on the network depends as much on you as on this team of professionals.
Just as you depend on your favorite mechanic to keep your car in working order while you take on the task of scheduling or carrying out a periodic oil change or tire rotation, a computer requires a partnership between the professionals and the operator.

Welcome to, or back to, RIT. ITS looks forward to partnering with you to make the RIT network a safe and relatively carefree place to carry out business, study and research.

Student Desktop Security Standards Introduced

By Ben Woelk, Information Security Office, ben.woelk@rit.edu

The scope of the Desktop and Portable Computer Security Standard has been revised to include student-owned or leased personal computers that connect to the RIT network. The revised standard is at http://security.rit.edu/desktop.html The standard requires users who are not supported by a systems administrator to:

1. Install **antivirus software**, keep it up to date, and scan their systems at least weekly. RIT provides McAfee antivirus software free for both home and campus use at (www.rit.edu/its/services/security/). Other brands of antivirus software are acceptable.

2. Make sure Operating Systems (Windows, Mac, Linux, etc.) are **up to date with patches** and **auto-update** turned on.

3. If it is available, install software that provides **buffer overflow (memory) protection**. McAfee Virus Scan 8.0i for Windows has built-in buffer overflow protection. (Buffer overflows are one of the most common attacks. Users who choose different antivirus software should make sure they provide buffer overflow protection.)

4. Use a **personal firewall**. Firewalls protect computers from outside intruders and also can prevent programs from inappropriately connecting to the Internet.
    a. For personally-owned or leased Windows computers, a good choice is ZoneAlarm (www.zonealarm.com).
    b. Macintosh users can use the built-in firewall in OSX.
    c. Linux users should choose an appropriate firewall.
    d. A hardware firewall can also be used to protect desktop computers.

5. Use **anti-spyware** (where available). Spyware sends personal information to other people without the user's knowledge. For Windows, Spybot Search & Destroy (www.safer-networking.org) and Ad-Aware (www.lavasoft.com) (free for personal use only) are good choices. It is important to use more than one product. Users can also use products from reputable vendors such as Microsoft, McAfee, Symantec, and Javacool Software. (Be careful of downloading other anti-spyware products. Some of them actually install spyware on your computer.) According to studies by the National Cyber Security Alliance and Earthlink, nine out of 10 computers are infected with multiple spyware programs, averaging about 26 spyware components each.

Note: *For RIT-owned or leased computers, users should contact the ITS HelpDesk to get information about the McAfee Firewall. Ad-Aware and ZoneAlarm are NOT free for RIT-owned computers. If products are not available from reputable commercial or reliable open source communities for a specific requirement, then the specific requirement is waived until an appropriate solution is available. For example, anti-spyware is not required or recommended for Macintosh at this time.*

Hold the Date: ITS Technology Seminar to Host Educause VP Cynthia Golden on October 24

By Michelle Cometa, ITS Communications and Public Relations Manager, Michelle.Cometa@rit.edu

The first ITS Technology Seminar features Educause Vice President, Cynthia Golden, editor of the recent E-Book, *Cultivating Careers: Professional Development for Campus IT* .Golden will

be on campus for a presentation on Tuesday, October 24, 11 a.m. – 1 p.m. Her session is about the special demands of continuing education and training for IT professionals within academic settings, how to succeed in cultivating current talent and creative ways to provide training for IT staff.

Cynthia Golden is responsible for professional development activities sponsored by Educause as well as the e-content and knowledge management initiatives of the organization. She also has general oversight of information technology services and strategies within the association. Golden previously held IT management and leadership positions, including the Chief Information Officer position, at Carnegie Mellon University, MIT and Duquesne University.

More information about registering for the session and the location is forthcoming.

Link for the e-book:
http://www.educause.edu/cultivatingcareers

About Cynthia Golden (with picture)
http://www.educause.edu/PeerDirectory/750?ID=02608

SIRP Redux: ID Replacement Project - Tying Up Loose Ends

Transition to New University ID Successful

By Bryan Meyer, ID Replacement Project Manager, Bryan.Meyer@rit.edu

The ID Replacement Project (alias SIRP) implementation was successfully completed at the end of May, 2006. This implementation transitioned the RIT campus from using Social Security Numbers (SSN) as the primary identifier for individuals, to the new University ID (UID).

With this transition the old RIT ID cards that contain Social Security Numbers, will no longer work on or off campus. The multiple computer systems that previously required SSN as the identifier now use University ID. An SSN is still required for legal, regulatory or government use.

The New RIT ID Card

Most faculty and staff members have picked up their new RIT ID cards from the Office of the Registrar. Students that were on campus for the summer quarter received their new ID cards at the end of the spring quarter. Students returning for the fall quarter received their new ID cards at check-in or, for those not in campus housing, at the Office of the Registrar.

Any faculty, staff or students that have not picked up their new RIT ID card will need to visit the Office of the Registrar to receive their card. Their business hours are Monday to Thursday, 8:30 a.m. - 5 p.m., and Friday, 8:30 a.m. - 4:30 p.m.

The new RIT ID card works in all the places the old ID card was used. This includes dining areas, vending machines, washers and dryers, and secured door access. If a card does not work, check first with the service provider. For example, for Food/Flex contact Food Service, and for door access contact your local administrator. If you're not sure who to ask, contact the ITS HelpDesk.

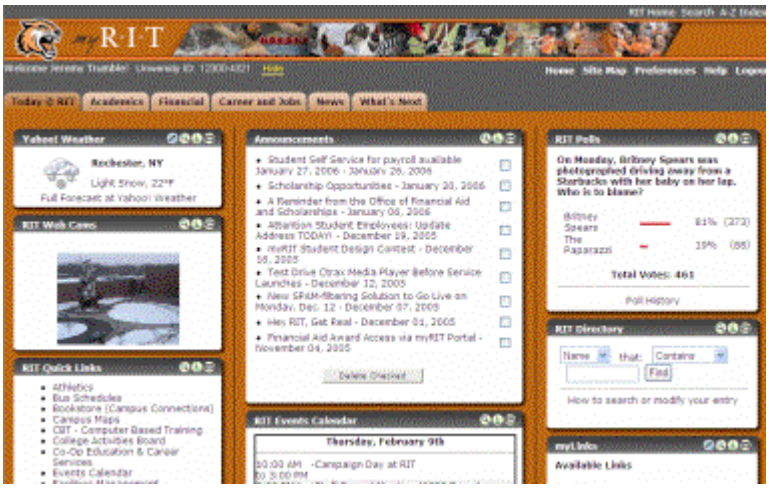
The Old RIT ID Card

The old RIT ID cards contain your Social Security Number. Anyone who has not already done so, must take the steps necessary to destroy, and securely dispose of, their old RIT ID card. The Office of the Registrar, and the ITS HelpDesk, will shred these cards, on request. But first, those that have Wallace Library copier funds on the old ID card will need to transfer these funds to the new ID card prior to destroying it. These funds actually reside on the RIT ID card. Tiger Bucks do not need to be transferred, as these funds are maintained on a university database.

The New University ID (UID)

For security reasons, University ID is not printed on the new RIT ID cards. It is encoded in the magnetic stripe and barcode on the ID card.

A common question being asked is, "How do I know what my University ID number is?" Individuals can locate their UID on the myRIT portal, which can be accessed at https://my.rit.edu . After logging in, UID is located in the upper left corner of the screen, and can be hidden or displayed.



The UID is also displayed on the RIT Employee Self-Service - My Personal Information and Contacts screen accessible at http://myinfo.rit.edu.

For those on campus in a service provider role, UID is available to those with STARS access and, with limited access, using the new CLAWS Lookup Tool.

Using Social Security Numbers At RIT

While the SSN is no longer used as a primary identifier at RIT, it is still required for government, legal and regulatory purposes. Employees, including student employees, are still required to provide their Social Security Number. Departments hiring students will no longer collect a Social Security Number from the student. They will only need to collect the University ID. The Student Employment Office will collect the student's SSN.

Financial Aid applicants will still be required to provide their Social Security Number. For Admissions, the SSN continues to be optional, and will continue to be required for anyone requesting Financial Aid.

Social Security Number will also continue to be required for payments to research participants, gifts, and other taxable payments. These are taxable events, and will continue to be tracked by the Accounts Payable department. Departments and Colleges will need to collect SSN from the receiving individual, and provide it to Accounts Payable, in a secure manner. The SSN *should not* be retained by the Department or College.

Data Security

Faculty and staff should review their existing electronic databases and other electronic data (e.g., files, email messages, etc.) containing personal identity information such as Social Security Number and name. All files (old, new, backups, archived, etc.) containing SSNs, that are no longer needed, should be deleted. Any files that must be retained for government, legal or regulatory purposes should be reviewed to eliminate all unnecessary personal data fields. If the information is required, ensure that it is adequately protected and in compliance with RIT Information Security standards. These are accessible at http://security.rit.edu/.

Ensuring the security of personal identifying information is important because it reduces risk of personal identify exposure and notification obligation. Under the new NYS Information Security Breach and Notification Act (effective Dec. 2005), RIT is required to notify New York State, and affected individuals, if certain combinations of personal identity data, in unencrypted electronic

form, are compromised or accessed by an unauthorized user (e.g.- a stolen laptop containing personal identity data).

Additional Information

The ID Replacement project website http://www.rit.edu/its/initiatives/sirp
contains a list of FAQs with additional helpful information, along with background information on the project.

Apple World Wide Developer Conference 2006: New Macintosh Computers with Intel Processors Showcased

By Jeremy Reichman, Sr. Desktop Support Analyst, jeremy.reichman@rit.edu

Apple's World Wide Developer Conference is a yearly event that brings together technical members of the Mac community—software developers and IT staff, among others—to learn about upcoming Macintosh hardware and software plans. RIT had the good fortune of sending four staff and having several students receive scholarships to attend this year. There were 4,200 registered attendees overall.

The conference started off on Monday, August 7 with a bang of new announcements in the keynote session. It continued for the rest of the week, jam-packed with sessions. Apple presented all the aspects of the technology incorporated into its products to benefit software developers as well as end users. In the course of the conference, I attended 20 sessions, as well as receptions that provided unfettered access to developers at Apple and other vendors. It's like cramming a whole academic quarter into a week. - JR

New computers
Apple introduced two new Macs with Intel processors. This completes their transition away from PowerPC.

The Mac Pro and Xserve replace the Power Macintosh G5 and Xserve G5, respectively. They both feature two Intel Xeon CPUs—each with dual cores—so that they have the equivalent of four processors. They are 64-bit processors, like the PowerPC G5, and designed with power efficiency in mind.

Mac Pro
The Mac Pro is a full-size tower system aimed at professional users who need the computing power of multiple high-end 64-bit processors. There are several improvements over the Power Mac G5, many owing to the roomier interior afforded by the removal of the prior computer's liquid cooling system. It can be configured with:

1. Quad 2.0, 2.6, or 3.0 GHz Intel Xeon 5100 processors
2. One or two DVD±RW drives
3. One to four hard disks
4. Up to four PCI Express cards.

For most office situations, ITS recommends a Mac mini or iMac instead of a Mac Pro.

Xserve
The Xserve is a rack-mountable server. The new Intel-based version moves to quad CPU cores at 2.0, 2.6, or 3.0 GHz. It adds lights-out management hardware and internal video support for more flexibility in more situations. The redesigned server also has more internal space that optionally supports a redundant power supply.

Mac OS X Leopard
Mac OS X 10.5, known as "Leopard," is slated for release in spring 2007. Until that time, Mac OS X Tiger is the newest version of the operating system available on our campus Apple Maintenance Program (AMP) agreement. When Leopard's expected release becomes reality, any RIT-owned computers on the AMP agreement are eligible for upgrades.

The following details were announced by Apple for Leopard (some are subject to change):

1. Time Machine is a new system component that makes versioned file backups to external disks or network file shares. Its interface presents your backups in time order, so it's easy to find previous versions of files—or a time when a file existed, if you deleted it in the interim.
2. iChat is slated to include screen sharing and application content sharing, in addition to its already impressive video conferencing abilities. Applications like Keynote and iPhoto were shown sharing presentations and photos, respectively, through a video chat session.
3. Window and information management takes a step forward with Spaces and Dashboard. The Spaces feature separates your windows into groups which act like virtual desktops to reduce clutter. You can make your own Dashboard widget from any portion of a Web page, and get live updates to it if it changes.
4. Accessibility changes improve the text-to-speech provided by VoiceOver, add more navigation options, and display closed captioning in QuickTime movies.
5. There will be 64-bit support throughout, including the application frameworks, in a single edition of the operating system that works on 64-bit Intel and PowerPC processors, as well as 32-bit systems.

We have to wait for more public announcements by Apple about Leopard, including its final ship date and system requirements.

Apple has not announced but we expect that Mac OS X 10.3 will no longer receive updates after the spring 2007 release of Leopard. Apple's trend is to issue security patches for only its current

operating system (i.e. Tiger) and the preceding major release (i.e. Panther). They have not released updates to Mac OS X Jaguar since Tiger shipped in April 2005.

RIT policy requires Institute computers to be kept up to date with security patches. Mac OS X system software cannot meet that requirement when Apple no longer releases updates for older versions. Therefore, your Macintosh computer should meet the system requirements for Tiger in the 2006-2007 academic year so that you can obtain Apple's security updates; for an evaluation, contact the ITS HelpDesk.

Information Security Office News: RIT and the NYS Information Security Breach and Notification Act

By Ben Woelk, Information Security Office, ben.woelk@rit.edu

The Information Security Breach and Notification Act, effective December 7, 2005, provides New York State residents with the right to know when a security breach has resulted in the exposure of their private information. You can read more about the act at http://www.oag.state.ny.us/consumer/tips/id_theft_law.html.

How does the Act impact RIT?
The Information Security Breach and Notification Act requires that RIT notify:

- Affected consumers following discovery of the breach in the security of computerized private information
- Consumer reporting agencies if more than 5,000 New York residents are to be notified.
- The Attorney General's office, the Consumer Protection Board and the NYS Office of Cyber Security & Critical Infrastructure Coordination of the timing, content and distribution of the notices and approximate number of affected persons.

What is a Security Breach?
A security breach is defined as an unauthorized acquisition of computerized data which compromises the security, confidentiality or integrity of private information. The loss of portable media, such as CDs, DVDs, USB memory, etc. constitutes a security breach if there is reason to believe private information may have been acquired by an outside or unauthorized party.

What is Private Information?
Private information means any personal information concerning a natural person in combination with any one or more of the following data elements: social security number, driver's license number, account number, or credit or debit card number in combination with any required security code.

What is RIT Confidential Information?
RIT Confidential Information refers to information that is accessed or communicated on a need to know basis that, because of legal, contractual, ethical, or other constraints, may not be accessed without specific authorization.

- It may have many forms including, but not limited to, documents, data, stored audio, or video.
- The classification "RIT Confidential" also applies to information the unauthorized disclosure of which could result in significant harm to the Institute, Institute processes, or to individuals.

What do I need to do?
You must treat all confidential data and information defined as private by the NYS Information Security Breach and Notification Act as *RIT Confidential Information*. Although the new University Identification Number and ID cards no longer contain Social Security Numbers, treat them as RIT Confidential Information.

What can be viewed as a potential security breach?
There are a few specific events that are potential security breaches requiring notification to affected parties:

- Whenever private information may have been disclosed
- Loss or misplacement of a laptop, PDA, Smartphone, or portable media, such as CDs, DVDs, USB memory, etc., containing unencrypted private information. (If you are reasonably sure that the information was encrypted or destroyed, the loss may not require notification.)
- Compromise or sharing of a password that allows access to private information and failing to change the password in a timely manner
- Discovery of certain types of malware, such as viruses, worms, spyware, keyloggers, back door/remote administration software on a computer containing or with access to private information. If you detect malware through a system scan, contact your HelpDesk for instructions.
- Email containing private information sent to the wrong addressee.

If you suspect a security breach involving RIT Confidential Information or Private Information, contact your HelpDesk AND Jim Moore, RIT Information Security Officer at 585-475-5406.

How should I handle RIT Confidential Information?

General procedures for handling RIT Confidential Information may be found on the Digital Self Defense 103 Web page at http://security.rit.edu/dsd_103.html.

Specific procedures for handling RIT Confidential Information are defined in your department's Information Access and Protection Plan. Contact your manager for information about the plan.

Student Self Service Available to Student Workers

By Christa Abugasea, Payroll and Kim Sowers, ITS Customer Support Services

RIT student employees are able to access many of the same self service transactions offered to RIT faculty and staff via the https://myinfo.rit.edu web site.

Using their Student Self Service account, students can

- View their current and past pay slips
- Review their W2
- Change their direct deposit banking information
- Change their W4 exemptions
- Verify their personal information on record in the Payroll department

It is important for students who currently have their paycheck directly deposited to a bank account to register for a Student Self Service account since paper deposit slips are no longer printed.

There are differences between Employee Self Service (ESS) and Student Self Service (SSS). One is that students self register within the Oracle Applications in order to create their SSS account whereas employees have their ESS account created for them as part of the new hire process. Students will need to enter their first and last name as it appears on their pay check when they create their SSS account. They will also need to know their employee number in order to create an account, which is also on their pay check.

While students will be allowed to create their own account name and password, the password they select will need to follow specific guidelines that are documented on the account creation page. Students can create only a single account to access Student Self Service. If a student forgets their password, they can go to the ITS Help Desk with their RIT ID card in order to obtain it.

Another difference is that students are directed to SIS to make personal information changes (e.g., address changes) since STARS is the system of record for student information. There isn't a real time update in place between Student Self Service and STARS at this time so students will not immediately see address changes made in SIS appear in Student Self Service.

Please encourage your student workers to take advantage of these on-line services. If your student employee has questions, they can contact the ITS Help Desk at 475-HELP, F&A Customer Support at 475-4905 or refer to the RIT Student Self Service Registration Process documentation available at http://finweb.rit.edu/controller/forms/studentselfservice.pdf.

Let's Face It! Social Networking on Facebook and MySpace

By Donna Cullen, RIT Digital Millennium Copyright Agent, Donna.Cullen@rit.edu

One of the advantages of youth is inexperience. Combine inexperience with exuberance, skill, a laptop, a digital camera and the new found freedom at a college campus – well, let's just say you have a formula for incredible accomplishment and experimentation.

You may be among the millions who have seen a preteen search the Internet for flight deals to her grandmother's or morph his friend into some sci-fi character worthy of Hollywood. Others are creating multimedia shows and PowerPoint presentations, writing software, managing their

own or their school's network. By the time a traditional student lands in college, they have been exposed to 12 or more years of computer usage – all during a time when they are very likely to feel uninhibited to try everything.

It is out of the college age group that many of the hottest computer hardware and software companies emerged. The inhibition of youthful minds is the fertile ground for great ideas and accomplishment. Higher education is all about exposing these minds to information, tools, ideas, people and experiences that enhance the innate skills and abilities students bring to the classroom, residence hall, event and laboratory.

One of the disadvantages of youth is inexperience. Combine inexperience with exuberance, skill, a laptop, a digital camera and the new found freedom at a college campus – well, let's just say you have a formula for incredible mistakes.

Music and movie sharing is one mistake many college students make. An "everybody is doing it" mentality prevails and for some it is just continuing a practice of many years. Some percentage of students sharing will face legal ramifications – notices, suits, civil fines or criminal penalties.

A student might discover that "private" digital photo of her body piercing on a web site. A fraternity might lose the chapter's charter when a public photo album displays members violating an Institute policy. Posting to the Internet is easy with the tools most students have at their fingertips and a portion of the student population sees no reason to moderate their own or their peer's Internet publishing.

Social networking such as blogs (web logs) has incredible potential in and out of the classroom. Imagine collaborating with world scholars about the newest nanotechnology or with car buffs about what to do with your stalling Mercedes.

Facebook and *MySpace* are two social networking sites that thrive off the exuberance of youthful subscribers. An individual creates a profile that typically includes a digital self-image, a self-description, some likes and dislikes, and other personal information. The individual can link to affinity groups or people with shared interests.

These sites have incredible positive potential. Students can "meet" a roommate before coming to campus or classmates once they are on campus. Students can introduce positive norms about everything from smoking avoidance to proper preparation for a high level calculus class to where to get the best second hand professional level cameras. Social networking allows an individual to interact online based on their interests or collaborate on research and projects. On a large campus, it has the potential of allowing a student to seek out people with like interests as a precursor to meeting in person.

Social networking online has the potential, along with the caching mechanisms, to permanently preserve a profile of an individual that brands them in an unfavorable light. Recruiters, law enforcement agencies, sports agents, and campus administrators are using Facebook and MySpace as means of profiling. These sites are open to anyone. Very private information is available to would be stalkers and others that would prey on individuals.

Some psychologists are concerned that for some individuals, digital interaction will replace in person interaction – causing a portion of the generation to lack the ability to interact in person.

Keeping in mind that a Facebook or MySpace entry is a “permanent” record, are you comfortable with your recruiter, employer, professor, colleague, or future partner seeing or reading your entry? Does your entry reveal information that allows a person to prey on you?

Social Networking is fun, exciting, and very now! Use it with a pinch of caution to unlock its incredible potential for networking across the campus and across the Internet.