ITS

ITS News Magazine

Winter 2005

The Official Source of News from Information & Technology Services

In This Issue...

Security Issue: Network Security in the Digital Age

Symantec Director Ariel Silverstone to Keynote Security Week
The third annual ITS Security Week technology seminars take place December 12-16 to increase awareness of identity theft and other online security challenges that affect individuals and systems.

File Sharing Myths and Truths
These myths are not unique to RIT but developed, enhanced and maintained by the millions of college-aged students using the Internet for illegal file sharing.

Student ID Replacement Project Update
Identifying the Impact of System Changes Related to International Students' Social Security Numbers

R·I·T

Contents

A Message from the CIO…..

Increasing Awareness, Reducing Risk

By Diane Barbour, Chief Information Officer

Each week the RIT campus is confronted with threats and potential compromises of critical Institute information stored electronically and in other formats. Known for its extensive use of technology, RIT is a prime target for criminals attempting to gain access to this information. The campus recognizes this risk, and has appointed divisional representatives to work with the Information Security Office to establish minimum security standards, which are the focus of the lead article in this issue of the ITS News Magazine (see page 3). The list includes standards for:

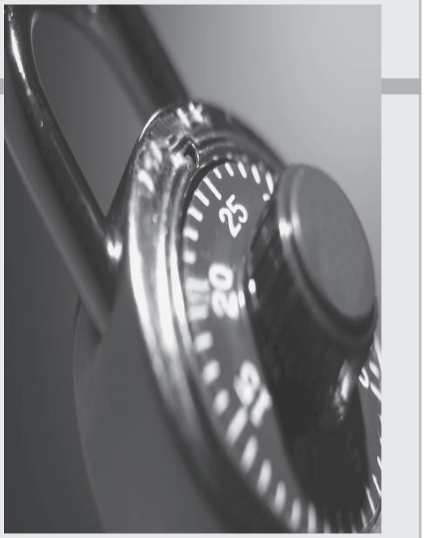
- Passwords
- Desktops
- Servers
- Computer Incident Management
- Information Access and Protection

Also contained in this issue are articles that cover anti-spyware, securing mobile devices, how to educate yourself on "safe surfing" and an article discussing the myths and truths of file sharing. By increasing your awareness of the risks in today's environment, you will be better prepared to reduce both your own personal risk and the risk of the Institute.

As a supplement to the information contained in this magazine, I also encourage you to participate in Security Week, which will take place the week of December 12-16.

Managing Information Risks: Information Security Standards

By Jim Moore, Information Security Officer



Each of us are important "risk managers" in handling, storing and maintaining the university's information assets which are confidential or critical to our core mission. Across campus we gather, use and store information in a multitude of ways. With that goes the responsibility to protect that information from threats that challenge our ability to protect its confidentiality, integrity and availability. In some cases, legal mandates (e.g., FERPA, HIPAA, Gramm-Leach-Bliley) specify what steps we need to take to ensure this protection.

So how does RIT's Information Security Office communicate this important responsibility and enable the RIT community to protect our information assets? One way we do this is by issuing Information Security Standards.

What's an Information Security Standard?

Information Security Standards are university-wide, baseline requirements (usage and technical) developed to meet current and emerging threats to RIT information availability and confidentiality. Standards may impact the way you gain access to network resources, the types of software you run on your computer, or how you handle RIT information. They may also codify existing best practices for many departments across campus.

Why does the Information Security Office (ISO) issue Standards?

It's one method for RIT to keep pace with the ever increasing threats, many of which enter the RIT community via the Internet. Standardizing the processes and practices we follow and the technical defenses we maintain brings a consistent level of information protection and attention. Standards will be reviewed and revised as needed to address the changing threat environment.

How are Standards created?

The creation and adoption of information security standards involves several steps: identifying the need for the standard, working with a small technical and business process *Core Team* to draft the standard, and then reviewing the standard with the ISO *Extended Team*. The cross-divisional Extended Team consists of representatives from both administrative and academic areas. After further legal and management review, the ISO issues the standard along with the communications and training materials needed to support its implementation.

Continued on page 20

SPAM Filtering Solution to "Go Live"

By Tom Dixon, Resnet, tom.dixon@rit.edu

In last month's edition of ITS News Magazine, ITS announced that we were close to implementing mySpam, an anti-SPAM service in conjunction with Symantec's Brightmail appliance. The service will be available to the general campus community beginning Security Week, December 12, 2005. Security Week was chosen for implementation because mySpam adds yet another layer of security to the RIT network. Many of the network security risks are sent through email. Phishing attempts, Trojans, viruses and backdoors among other exploits can be found in SPAM messages. By reducing the amount of SPAM, we reduce the risk. ITS will be providing a general overview of mySpam during Security Week. These seminars will be held Monday, December 12, 12:00 -2 p.m. in the Idea Factory at the Wallace Library and on Thursday, December 15, 4-6 p.m. in the Xerox Auditorium in the College of Engineering.

mySpam is a service that will filter email messages that show a high probability of being SPAM. These messages will be held in quarantine for 14 days, during which time you may view them, release them to your inbox, or ignore them and allow them to be deleted automatically.

SPAM inundation has been the number one concern according to users in the ITS Customer Satisfaction Surveys for the last several years. In response to this concern, ITS has been working diligently to limit the amount of SPAM entering your inbox. SPAM is not only annoying it may also be dangerous to your computer and the RIT network. By implementing this service, we hope to accomplish three things: to better secure the RIT network, to protect workstations and to reduce unneeded traffic on the network. Each of these things translates into a safer, more productive campus computing environment.

How does it work?

The service will scan each message destined for your inbox. In the process, it has been configured to do one of three things:

1. mySpam may see the message as a positive SPAM match meaning that it has every confidence it is indeed SPAM and will automatically filter the message out. This includes pornographic email, unsolicited sales pitches, etc.

Continued on next page

2. mySpam may see the message as potential SPAM, sending the message to quarantine. The message will remain in quarantine for 14 days, at which time it is deleted. You will receive a report each day from mySpam detailing any messages that were sent to quarantine. You may then ignore those messages, and they will be deleted automatically in 14 days. Or, you can release them to your inbox if you believe they are legitimate emails.

3. mySpam may see the messages as normal emails and allow them into your inbox.

What if I want to make changes to my personal filters?

Yes, you can change your configuration by logging into your mySpam page. Your mySpam page will be available through a link provided in your daily mySpam report. In the configuration, you can block messages from specific senders, allow certain types of messages through, or unfilter certain senders. This can be your call!

Are there false positives? I don’t want to lose mail!

As with any system there is the possibility of a false positive, however, through our extensive testing we have found this to occur only a few times over the course of numerous messages. After reviewing several products from several vendors, this product had the lowest number of false positives and was the most reliable. (According to vendor documentation, false positives occurred in 1-in-1 million messages. More information can be found at: http://www.symantec.com). You can be confident in the system, and it will serve you well.

mySpam service is expected to eliminate more than 99% of all SPAM messages entering your inbox. By reducing the amount of SPAM, yet another layer of security will be added to the RIT network. If you have any questions regarding the implementation or functionality of mySpam, please contact the ITS HelpDesk at 475-HELP (4357) or 475-2810 TTY.

Spyware Fight Gets Tougher by the Day

By Susan Barnes

© *Reprinted with permission of the Rochester Democrat and Chronicle*

Who would think that a friendly smiley face could be a facade for malicious activities?

Well, that's what I discovered while writing last week's column. It took me longer to find out because I use a Macintosh and the spyware that downloads with smiley faces targets Windows machines.

Spyware has been described as the "bane of the Internet" and it is also referred to as trickware. These are software programs that install on your computer without your knowledge or consent. In some cases spyware will not enable you to install the software you want, like an animated smiley, without installing something else.

That "something else" is software designed to do several things. Software will collect data about you and store the information in a database. Others will sell, rent, give away, or share information it has collected from your computer without your knowledge or consent.

How is spyware installed on your computer? This is where the "trick" in "trickware" comes in. Spyware can install itself through pop-up ads. When you click "OK," the spyware downloads and when you click "CANCEL" it also downloads. Sometimes even clicking the "X" to close the window will download spyware. Whatever you click seems to download the program.

There's no free lunch on the Internet. If you see something being offered for free, it probably comes with the price of spyware. Rochester freelance writer Joy Underhill says, "I once downloaded some smiley faces and was horrified at the amount of spyware that was downloaded with it."

Thundercloud.net warns that The Excite Group, a large publicly traded company, runs a site call Smiley Central that is full of spyware. You can't install Smiley Central without adding spyware to your machine. They also advise users not to believe sites that state "NO SPYWARE, NO POP UPS, NO SPONSORED LINKS." If you have downloaded Smiley Central, removal instructions can be found online at:

www.pchell.com/support/smileycentral.shtml

Continued on next page

Smiley Central promotes itself as an "Internet Explorer plug-in that allows you to add numerous smiley faces to your e-mail or instant messages." Its parent company, The Excite Group, has a suite of utilities marketed under the brand Fun Web Products. These products contain spyware. Spyware tactics used by The Excite Group and others have now come to the attention of the Federal Trade Commission.

New spyware programs are being released every day and users must be vigilant and keep spyware prevention tools up-to-date. Although Windows software is more often a target for spyware than Macs, I'm still keeping all my virus programs and Apple security downloads up to date. You never know what types of gimmicks spyware tricksters will use.

This article was printed in the September 25, 2005 issue of the Democrat and Chronicle. Susan Barnes is a columnist for the local newspaper, writing about online technology issues and information. Her columns can be found regularly in the Sunday print newspaper as well as the online version. Barnes is also a faculty member in the College of Liberal Arts, Communications Department.

File Sharing Myths and Truths

By Donna Cullen

Did you know that a pedestrian tunnel exists between the residential and academic sides of campus?

If you became a freshman on the RIT campus during the early 1980's, you heard this myth. You probably were instrumental in keeping it alive by passing it off to the next "newbie" you met.

Persistent in the telling, this myth was still around when the 80's became the 90's. The myth became "truer" as it was repeated in computer conferencing systems at a time when the "if it is on the computer, it is true" mentality existed. Except for the embarrassment felt by the latest freshman asking for directions to the non-existent tunnel or pleading with the President to open the tunnel during the freezing Rochester winter, the tunnel myth held little harm for the believer.

The RIT tunnel myth has been replaced by a new mythology - the file sharing myths. These myths are not unique to RIT but developed, enhanced and maintained by the millions of college-aged students using the Internet for illegal file sharing. As with many myths, the number of believers has caused the myths to take on a life that persists beyond logic and truth. Some of the examples of the myths as they are adapted by RIT students:

The No One Suffers Myth

Students are not hurting anyone by sharing music (or other copyrighted material).

Truth – Without discussing whether *KISS* or *Madonna* are hurt when music is illegally shared or *Universal Studios* loses revenue when a movie is shared pre-release, the person most likely to be a victim of the file sharing is the student sharing the material. It is the student (not the university) that is held liable for the damages. Parents of underage students (those under 21 years of age) are also held accountable. Students named in recent subpoenas found themselves in need of legal counsel. A copyright violation conviction is a felony that can result in a combination of jail time and large fines. Students who enter a plea in federal court also face judicial action at RIT.

Continued on next page

The Big Fish Myth

The only student ever sued by the RIAA is the person who is sharing thousands of titles of the latest music.

Truth – The subpoenas are not targeted specifically at those who share “new” materials. Nor are the subpoenas targeting only people with large file shares. If you are sharing materials illegally, you can be sued.

The Intranet Myth

RIT is aware that students run music servers on campus. RIT condones any server that restricts traffic to on-campus sharing.

Truth – RIT does not condone illegal file sharing. RIT shuts down any illegal file server it finds and seeks sanctions for both the person who registered the server and the people found using the service. Such servers are typically found as a result of a report to support staff or an unusually high amount of network activity. In some cases, the insecure nature of peer-to-peer sharing software results in the server being corrupted and in the course of eradicating the compromise, the illegal activity is identified.

The Sanction Myth

RIT does nothing with reports of illegal file sharing.

Truth – RIT contacts the person associated with each copyright infringement notification. The machine associated with the violation is removed from the network and the person referred to the RIT judicial process if the student does not immediately remove the infringing material or the student is a repeat offender.

The Fair Use Myth

If I purchased a CD or a music track, I can make unlimited copies of it and I can put the music on a shared area of my computer.

Truth – The purchase of a CD or music track entitles you to make a copy for yourself in a different media. It allows you to turn ownership of the original (and all copies) to another person. It is illegal for you to make a copy for your dad, big sister, roommate or anyone else. It is also illegal for you to put that music in a shared folder on your computer and open the share to *anyone* other than you.

Continued on page 28

Securing Your Mobile Devices

By Nathan Fisk

For those who need constant access to their data, there are few solutions that can top the convenience of a handheld device. But with convenience often comes new security threats, and handhelds are no exception.

As mobile devices become more popular, they create a larger target for attackers and thieves. There is a rapidly growing market for all different types of data, from social security numbers to trade secrets, all of which can be easily stored on a handheld device.

Furthermore, handhelds are rarely designed with security in mind. They are generally insecure without additional software and security settings. Following a few common sense guidelines can help keep your data and your mobile device safe.

Keep Your Handheld (Physically) Safe

Handhelds are so convenient precisely because they are so easy to pick up and carry. Unfortunately, this means that someone interested in your handheld can grab it and leave just as easily as you can. Make sure you know where your handheld device is at all times. Make sure you store it in a safe place in the office, at home and on the road.

Restrict Access to the Data on Your Handheld

If your handheld device is stolen or lost, anyone who has it can easily gain access to all of the information stored on it, including e-mail, contacts and documents. If your device supports it, be sure to set a power-on password and change it regularly.

There are also a number of encryption programs available for the different types of handheld devices (Palm/WinCE/Blackberry). Using one of these encryption programs ensures that even if someone bypasses your power-on password, the data your handheld contains cannot be accessed. If you carry *any* confidential information on your handheld, encrypting that information is highly recommended.

Secure Your Wireless Connections

More and more handhelds are being used to access data wirelessly in some form, either through Bluetooth, 802.11 networks or cellular networks. When you aren't using these features of your handheld device, just shut them off. Disabling 802.11 and Bluetooth will not only prevent people from accessing your device without your knowledge, but will also increase your battery life.

When you do use these wireless capabilities, you may be opening your handheld to a number of attacks. Make use of both a firewall and Virtual Private Network (VPN) if you access RIT e-mail via your handheld device. VPN will ensure that your wireless traffic cannot be intercepted by someone "listening in" to the network, and the firewall will prevent attackers from accessing your device wirelessly.

Continued on next page

Backup Your Data

No security plan is perfect, and there is always a chance that your mobile device will become breached in some way. Many people do not realize the importance of the data they stored on their handheld device until it's gone.

How valuable is your calendar, or your contact list? How much time would it take to recreate them? By backing up your data, you can not only ensure that you always have access to the information you need, but also that there is a record of what information you had stored on your mobile device if a security incident occurs. Luckily, backup functionality is standard on most handheld devices. Check your user manual, and make sure you know how to backup and restore data on your device.

Keep Viruses Out

Finally, run anti-virus software on your handheld device, and make sure you keep up with software patches. While viruses are not a significant threat for handhelds at the moment, they could be used to carry viruses to your PCs. As handhelds become more popular, you can expect to see viruses that specifically target them as well. Running anti-virus software and keeping up to date with patches will protect your handheld against such a threat.

While these guidelines will help mitigate some of the risk involved in using a handheld, keep in mind that no solution is perfect. If possible, avoid storing any confidential information on your handheld at all, including any confidential e-mail. If you do, and the handheld is lost, stolen or breached in any way, recent New York State laws require that the users whose confidential information was on the device must be notified. So, think twice when you put any sensitive data on your handheld.

Remember: keep your handheld safe, encrypt your data, encrypt your network traffic and backup your device. With these guidelines in mind, hopefully you can have the convenience of a handheld without the inconvenience of a security breach. If you have any questions about keeping your handheld secure, e-mail the Information Security Office at infosec@rit.edu.

Nathan Fisk is a research assistant in the Information Security Office. He is a graduate student in the Communications and Media Technologies program in the Communications Department of Liberal Arts. He also has been a part of the research team with Professor Sam McQuade who has been studying the issue of illegal file sharing online.

Student ID Replacement Project Update

Identifying the Impact of System Changes Related to International Students' Social Security Numbers

By Dave Pecora and Bryan Meyer

Ongoing Student ID Replacement Project (SIRP) Task Force meetings give participants the opportunity to address concerns about the vast student systems changes that will take place in spring. The project is being conducted in a phased approach:

- **Phase I** – Identifying the Impact
- **Phase II** – Planning for the Conversion
- **Phase III** – Developing Action Plans

Each phase is elemental, with each of the different departments and college groups identifying the methods they use to categorize student information and records, distinguish what will be transitioned and what aspects must continue to use social security numbers in records as required by law or accrediting agencies.

The project is in its first phase with the Task Force group assessing their individual business processes. Some questions that have been brought to Task Force meetings of late have been helpful in raising the awareness of specific scenarios about how groups use the Social Security Numbers (SSNs) – and how these processes will need to change.

Here are several of the recent topical questions:

Some groups have heard that they cannot call ITS during the process freeze which began October 3, 2005. Is this true?

A hold, or production freeze, on systems changes was put in place on October 3 as a way to have ITS Student Systems staff prepare for, and develop fully, the new transition infrastructure. However, error correction maintenance is being done for production issues; the scope and impact of these errors is being evaluated to determine if modifications need to be completed immediately or can be held until after the "freeze" (Feb. 2006). All production needs related to federal policy and financial aid requirements, for example, will be addressed through the freeze. Anyone with questions about which of their respective processes fall into the categories above can call the ITS representative they work with for clarification.

Will the social security-style numbers given to international students also be converted to the new University ID?

International students were given a 999 or 990-xx-XXXX number upon arrival at RIT. This number was a means of both categorizing this population of students as well as integrating them into the main student records system database. This number is not a formal SSN, but was put into the SSN data field on records for the individual student. All data in these fields will be transitioned and instead of an SSN, international students, like their American counterparts will have a University ID.

Some departments have student mail boxes in public areas and individual folders in the mail boxes have student names and SSNs. Shouldn't these be changed?

Yes, the folders with this information should be changed especially if the folders are in public areas. This is one of several "process" changes that need to be addressed in the preliminary stages of this project.

The Task Force group will continue to meet and address questions such as those raised here, even those considered exceptions. Questions can be forwarded to Task Force members to bring to upcoming Task Force meetings or they can be sent to the Task Force mail list: ITSSIRPTaskForce@rit.edu.

Bryan Meyer is the project manager for the SIRP project. He oversees the technical and logistical aspects of this vast project as well as coordinating the Task Force meetings. He can be reached at bryan.meyer@rit.edu. Dave Pecora is the Associate Director of ITS Customer Support Services and manages the ITS HelpDesk and its main support functions. He is the communications coordinator for the SIRP project, coordinating different informational aspects of the project. He can be reached at dave.pecora@rit.edu

digital
self
defense
Protect yourself and everyone else

Martial Arts and the Internet

By Ben Woelk

How do you help ordinary people defend themselves against:

- Internet-borne threats to information assets, both personal and professional?
- Threats that are increasing rapidly, both in number and complexity?

You provide lessons in Digital Self Defense!

The Information Security Office staff developed *Digital Self Defense 101* (DSD101) to introduce people to the types of attacks they face from the Internet and provide them with the "self-defense" training they need to recognize and defeat these attacks.

DSD101 provides an overview of the different methods of attack. It introduces attendees to technical solutions and commonsense practices that equip them to protect both RIT's and their own information assets. We talk about the need for patching, using anti-virus, firewall, and anti-spyware. We also introduce attendees to social engineering attacks—helping them recognize scams, phishing attempts, and other attempts at identity theft.

DSD101 has proven to be very popular. More than twenty sessions have been held since January 2005 and almost 400 members of the RIT community (including faculty, staff, and students) have attended. DSD101 is held several times each quarter and several departments have asked us to present special sessions to their faculty and staff.

DSD 102, the next level of training classes, provides instructor-led, hands-on practice using the security software and practices required by the RIT Desktop and Portable Computer Standard. The classes are designed especially for participants who need a confidence boost before installing and using recommended or required software, whether at RIT or at home. Topics include patching, firewalls, anti-virus, and anti-spyware. DSD102 classes are scheduled several times each quarter. A list of the next series of Digital Self Defense classes can be found on the Information Security website: http://www.rit.edu/infosec

Ben Woelk is the communications coordinator for the RIT Information Security Office team. He is often the trainer for the Digital Self Defense courses conducted on campus, both the 101 and 102 series. He will be a featured presenter at the ITS Security Week program, presenting a Digital Self Defense workshop and participating at a hands-on session to patch individual computers.

Symantec Director Ariel Silverstone to Keynote Security Week

By Patrick Saeva and Michelle Cometa

December Program Highlights include Identity Theft Prevention, Online Challenges for Residential Students and Legislation for Higher Education

Higher educational institutions have been targeted by hackers for many reasons, not the least of which is the vast store of personal data. From social security numbers and credit card information to system passwords or PINS, the data is a gold mine for identity thieves.

The third annual ITS Security Week technology seminars take place December 12 through 16 to increase awareness of identity theft and other online security challenges that affect individuals and systems. Each year, the series highlights some of the most talked about issues in network security – wireless security, filtering SPAM, online challenges for residential students and legislative issues.

This year's keynote speaker is **Ariel Silverstone**, Director of Strategic Consulting and former Chief Information Security Officer for Temple University. He will present Security Threats in the Digital Age and Effective Solutions for Secure Data Systems on December 12 at 3 – 5 p.m. in the Golisano College Auditorium. After this session, ITS will host a reception with Mr. Silverstone in the Golisano College Atrium, just outside the Auditorium, from 5 – 6 p.m..

As in the previous years, presenters are from campus and local colleges. **Steve Schuster**, Director, Information Security, from Cornell University presents, "Security Incident Response in light of Legislation Affecting Higher Education." In the last several years, the legislature has proposed and enacted laws on disclosure and privacy.

California was the first to enact a law about disclosing when an organization's system is hacked and letting customers know of this exposure. Many other states have followed suit, and in fact, New York State also has enacted legislation in this same vein. RIT and other colleges are expected to comply with the disclosure statutes. To do so, they will have to have internal policies and practices in place; Shuster will describe how colleges will be able to comply successfully. His session is a must for those who oversee the many databases and systems RIT uses every day.

Continued on page 19

ITS Security Week December 12-16

Security Week Seminar Lineup

Security Week sessions are free and open to all students, faculty, staff, and administrators.

To register for Security Week workshops, send email to cioits@rit.edu with the individual workshops you will be attending. Interpreters are available upon request.

Monday, December 12

Brightmail: SPAM Filtering Solution
Presenter: Tom Dixon, ITS, Resnet
Noon – 1 p.m., The Idea Factory, Wallace Memorial Library

This session is about the new SPAM-filtering solution and how to effectively decrease more SPAM in email accounts. Learn how to use the software, how messages are quarantined and how to release authentic messages to your mail box or delete nuisance SPAM messages *before* they get to your account.

Keynote Presentation: Security Threats in the Digital Age and Effective Solutions for Secure Data Systems
Ariel Silverstone, Director of Strategic Consulting
Symantec Corporation
3 – 5 pm, Golisano College Auditorium

A leader in the corporate security industry, Symantec provides a variety of services to help organizations and end users protect sensitive data on their networks. Mr. Silverstone will discuss the challenges today to secure personal data, the trends in security breaches and the solutions that organizations, especially higher education, have integrated to secure networks.

A reception will follow this presentation from 5 – 6 pm in the Atrium of the Golisano College.

Continued on page 16

Security Week Seminar Lineup *continued*

Tuesday, December 13

Security Incident Response in Light of Legislation Affecting Higher Education
Steve Schuster, Director, Information Security, Cornell University
9:30 – 11 a.m., 76-1125

> This program will cover the emerging state and national laws being enacted to protect against identity theft and the specific challenges these laws pose for higher education. Learn about some of the requirements expected from colleges and universities about disclosure, staffing requirements and compliance.

PANEL Discussion: Protecting Students from ID Theft in a College Environment
11:30 a.m. – 1: 30 p.m., 76-1125
Panelists: Joe Lofreddo, RIT Registrar; Dave Pecora and Dan Tobin, ITS; Jim Moore, Information Security; John Zink, RIT Risk Management & Safety Services
Moderator: Professor Nick Francesco, College of Business

> Bring your lunch and join this group of panelists as they discuss the specific steps and safeguards they have put in place to better secure the vast amounts of personal data required of a university network. Each will present their perspective about data access policies, compliance measures and disclosure requirements – all necessary parts of their roles as data stewards.

The Nexus of Cyber Ethics, Information Security, and IT-enabled Abuse and Crime
Samuel McQuade III, Professor, College of Liberal Arts, Criminal Justice Program
2 – 4 pm, 76-1125

> This presentation features empirical findings from a series of computer use and ethics surveys conducted at RIT from April 2004 through May 2005 to draw connections between levels of cyber ethics beliefs, information security knowledge and skills, and IT-enabled offending behaviors by college students.

Continued on next page

Wednesday, December 14

Computer Forensics
Bill Stackpole and Yin X. Pan, Professors, Golisano College of Computing and Information Sciences
9:30 – 11 am, Golisano College Auditorium

> Computer Forensics is the term used for investigating computer systems for evidence of mis-use or computer crime. The presenters will describe how investigations are done, and will include information about existing tools used to recover data on both Windows and Linux platforms.

Digital Self Defense 101
Ben Woelk, Information Security
12 – 1: 30 p.m., Xerox Auditorium, Kate Gleason College of Engineering

Identity Crime
Steve Petro, Resident Agent-in-Charge, Social Security Administration, and Rodney G. Lezette, Jr., Investigator, RIT Campus Safety Department
2 – 4 pm, Golisano College Auditorium

> This presentation is about how identity thieves adopt another person's identity to defraud them, by purchasing goods, services or obtaining credit without their knowledge or consent and/or facilitating other criminal activity. Learn more about how this is done, how individuals are vulnerable and how to decrease the likelihood that you would be a victim of identity theft.

Mary Beth Cooper
Vice President, Student Affairs

© photo by Sue Weisler, University News

Thursday, December 15

Online Challenges for Residential Students
Mary Beth Cooper, Vice President, RIT Student Affairs Division
9 – 11: 30 a.m. 76-1125

> Dr. Cooper will discuss the social implications of technology in a residential setting, as well as the challenges of building community on college campuses and the role technology plays, including Student Affairs' response to peer-to-peer file sharing issues.

Continued on next page

Security Week Seminar Lineup continued

Thursday continued

Wireless Security
Bruce Hartpence, Professor, Golisano College of Computing and Information Sciences
1 – 3 pm, 76-1125

What are the challenges of securing wireless networks? What are the trends in wireless technology that must be addressed on campuses with the increase in wireless devices? Learn answers to these and other questions related to wireless security measures in this session.

Cyber Security Tips During the Holiday Season
Broadcast Session, 3-4 p.m, 70-1400

Brightmail: SPAM Filtering Solution – Student Session
Presenter: Tom Dixon, ITS, Resnet
4- 6 p.m., Xerox Auditorium, Kate Gleason College of Engineering

This session is about the new SPAM-filtering solution and how to effectively decrease more SPAM in email accounts.

Friday, December 16

Securing Your Laptop Computer
Ben Woelk, Information Security Office
10 a.m. – 12 p.m., Location: TBD

Bring your laptop computer to this session and learn about the resources available to campus users, most current updates and patches necessary to comply with RIT network standards and how to continually update laptop computers over time.

symantec.™

Symantec Director Ariel Silverstone to Keynote Security Week

Continued from page 14

Several presenters will make return engagements to Security Week: **Steve Petro**, Resident Agent-in-Charge, Social Security Administration, from Buffalo, New York will reprise his session on Identity Theft–how personal data is mined by identity thieves and what an individual needs to do for protection. He will be joined by Rod Lezette of RIT Campus Safety, for their session on Wednesday, December 14 from 2-4 pm.

New to the line up will be **Mary Beth Cooper**, Vice President of Student Affairs. She will present information about "Online Challenges for Residential Students." In the last several years, students have been targeted by the Recording Industry Association of America (RIAA) for illegal file sharing. This population of students is one of the most "connected" and on any given day, they can be seen chatting on cell phones, checking email on Blackberry wireless devices or jamming to tunes on their IPods. Their expectations of online services have prompted many colleges and universities to increase network capabilities and provide more access to online functions–but with what additional challanges?

One of the highlights of the week will be a panel discussion about "Security for Student Systems in Higher Education" moderated by College of Business professor **Nick Francesco**. Participants from RIT will discuss challenges of system safeguards on Tuesday, December 13. This will be a "brown bag" lunch session from 11:30 am – 1 pm in the CIAS Auditorium, 76-1125.

Two hands-on sessions also are taking place with participants able to learn more about how to use the Brightmail SPAM filtering software offered at RIT and how to secure laptop machines. Brightmail is a recent addition to the collection of filtering solutions to reduce nuisance SPAM. *(See separate article about this application in this issue on page 4.)*

To register for the workshops, or for more information and to secure interpreting services, contact cioits@rit.edu

Managing Information Risks: Information Security Standards

Continued from page 3

How does the ISO Ensure the Standards are right for RIT?

The ISO assesses the information security threat environment and assigns risk factors appropriate to our university operations. We also conduct benchmarking of higher education best practices along with existing best practices within RIT's colleges and divisions. The expertise of the *ISO Extended Team* also benefits the ISO in standard development by helping achieve the most effective implementation strategy for each standard.

What are the current ISO Standards?

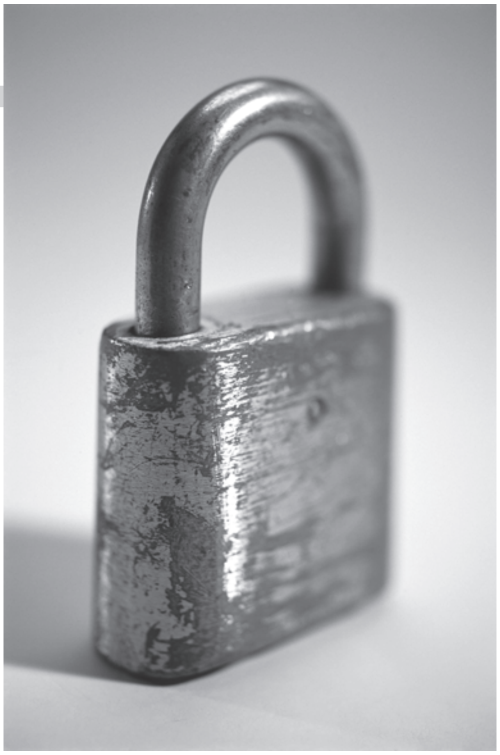
The standards, compliance dates, audiences and impacts are outlined below.

Standard	Compliance Date	Audience	Impact
Password	6/30/2004	**Entire RIT Community**	Requires use of secure passwords changed every 120 days. End users are responsible for their RIT account passwords. Authentication Service Providers are responsible for RIT system passwords.
Desktop	6/1/2005	**Users of RIT-owned or leased computers**	Requires the use of protective practices and software including patching, antivirus/buffer overflow protection, personal firewall, and anti-spyware. Primary responsibilities belong to administrators of RIT-owned or leased computers. The administrator may be the end user or the system administrator.
Server	11/15/2005	**Systems Administrators (SAs)**	Establishes minimum security server configuration and supporting documentation. Systems Administrators (SAs) will have increased responsibilities in ensuring servers meet security requirements.
Computer Incident Handling	11/15/2005	**Entire RIT Community**	End users should report potential loss of information or devices containing information to their Systems Administrators (SAs) and Information Security Coordinators. Primary responsibilities belong to Systems Administrators (SAs) and Information Security Coordinators who will need to follow a specific incident handling and reporting process.
Information Access & Protection	12/15/2005	**All RIT Managers**	Promotes consistent identification, handling and storage of RIT sensitive information ensuring confidentiality and integrity. Each department manager will develop a written plan.

Continued on next page

What steps should be taken if I can’t come into compliance by the compliance date?

Each standard allows for an exception process should compelling business reasons prevent you from achieving compliance. You should file your exception before the compliance date of the standard. Your compliance with each ISO standard is subject to review by the RIT Information Security Officer, as well as the Institute Audit, Compliance and Advisement Office. Findings of non-compliance outside of the exception process will lead to appropriate management notification and follow up.



What new ISO Standards are planned for development this academic year?

While changing threats may alter the current ISO development plans, the following topics will be addressed in the coming months:

- Network Standard (network protection requirements)
- Mobility Standard (requirements for use of mobile devices such as PDAs and thumb drives.)
- Instant Messaging Standard (requirements for use of Instant Messaging)

How does the ISO help the RIT community comply with these Standards?

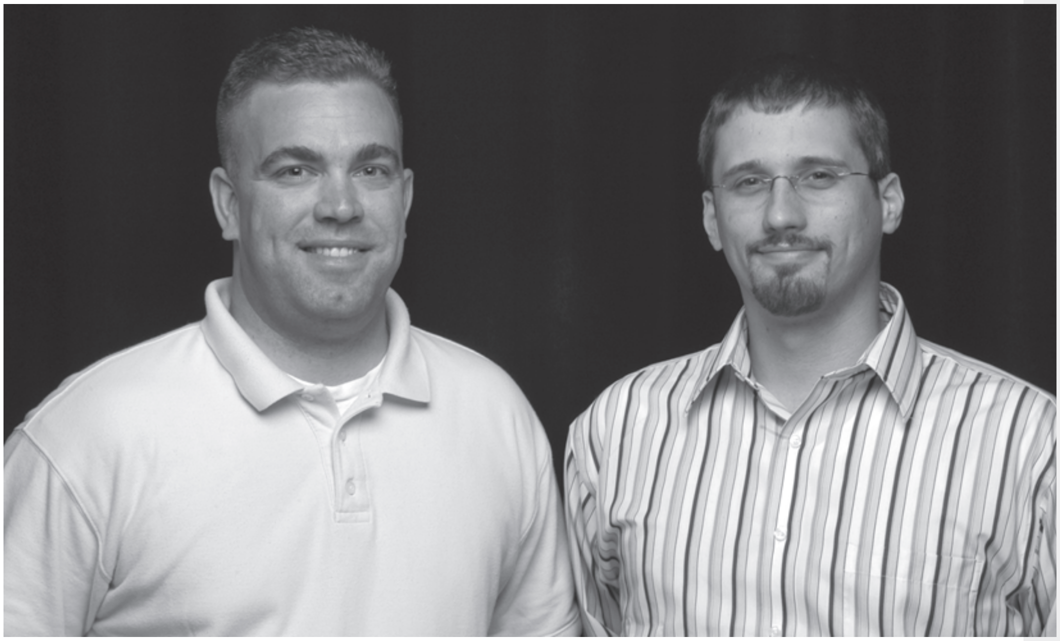
We help by:

- Releasing “Plain English Guides” for each standard to provide a non-technical, snapshot view of the purpose, audience, scope and action steps necessary for compliance.
- Providing education and training, such as Digital Self Defense workshops, manager orientation sessions, and compliance-specific workshops.
- Developing job aids and tools that support compliance measures.
- Promoting interdepartmental communication of best practices and other efficiencies to achieve effective use of resources.

Where can I go to learn more about ISO standards and the various workshops and resources designed to assist me in compliance?

More information about each standard, including workshop offerings and schedules can be found at:

http://security.rit.edu/standards/



Resnet Staff Nominated for Staff Council Customer Service Award

Dan Swab and Tom Dixon, staff of ITS Resnet, the residential computing service, were nominated for this year's Staff Council Staff Recognition Awards. They were nominated in the Group-Customer Service division for their work with students based in residence halls on campus.

Dan and Tom can be found at the Resnet Office located in Nathaniel Rochester Hall. The customers Resnet serves are on campus students living in the residence halls and apartments. Students look to Resnet to provide support for their networked computers, from various services, software installation, repairs and ongoing information about keeping their systems safe. They are the frontline defense for both the student computers and the student users. The Resnet team must advocate for students and protect both them and the RIT network from the many viruses, worms and other network problems. The Resnet team was established nearly 10 years ago, and since that time it has grown to be one of the strongest, student-centered teams on campus and in ITS.

© Photo of Tom Dixon, left, and Dan Swab, right, used with permission from the Educational Technology Center

ITS Staff Member, Nancy Simonds, Wins 2005 Regional PTA Leadership Award

Nancy Simonds, senior programmer/analyst in Information and Technology Services (ITS) was recently awarded the Ruberta Foster Leadership Award from the Genesee Valley Region PTA. She is a long time member of the Greece Athena High School PTA and is currently serving as Associate Director for the Genesee Valley Region PTA.

Simonds was instrumental in developing and coordinating an extensive training model, called the Leadership Academy, for new PTA members across a six county region. The training sessions are intended to orient new PTA board members about service requirements and procedures for their tenure with local and statewide PTA organizations. In the last several years, the training sessions were presented locally and within the six counties the Genesee Valley Region PTA serves. “We revamped the [training] process and took it on the road,” she said recently. The programs served to increase participation as well as retention of members.

“I was very surprised and honored about receiving the award,” Simonds said. She was not aware she was nominated, but her 16-plus years of service to the Greece School District and on the regional board was appreciated by many. Through her time with the PTA, she served in all the leadership positions from treasurer through president of the Greece PTA.

The Ruberta Foster Leadership Award has been given out since 1984 in recognition of PTA leaders to honor leadership qualities exemplified by Foster during her tenure with the PTA. The award is given at the annual Presidents’ and Principals’ Dinner, the most recent on November 2, 2005 at Logan’s Party House in Rochester, NY. It was attended by more than 200 principals and PTA leaders.

Nancy Simonds is a member of the ITS Student & Development Systems group. She celebrated 25 years with RIT recently.

Profiles in CO-OP

By Dianne Parker, Distributed Support Services, dianne.parker@rit.edu

Each month, ITS News features profiles of the co-op students who work within our Division. This month our featured co-ops are ***Minh Luong*** *and* ***Andrew Wurster.***

Minh Luong is originally from Ho Chi Minh City, Vietnam. He and his family immigrated to the United States and now reside in Rochester, NY. He lives with his parents, an older brother and a younger sister. He is a fourth year student in the Management Information Systems (MIS) program in the College of Business.

When Minh was deciding what to go into at college he selected business. However, he thought some knowledge of IT would help him so he decided to study MIS, which he considers a blend of both worlds.

Minh's current position in ITS is Computer Lab Operational Assistant. This position oversees management and operation of seventeen computer labs across campus. He chose to work at ITS for several reasons. He feels that the position fits his major very well. He can practice management and still have a chance to apply his IT knowledge.

Minh says of his ITS co-op, " I enjoy this co-op very much. I have learned a lot. I would recommend MIS majors doing their co-op at ITS because this job is a great match for our major." The thing he considers the most interesting about his co-op is the diversity of the staff. In his free time Minh likes to play tennis and swim.

We really enjoy having Minh as part of the ITS team.

Our second featured co-op is **Andrew Wurster**. He says where he is from, "there are no political boundaries." When not at RIT, he lives with his parents and one younger sister, Eleni, "the one with the cool name." He is currently a third year student in the Information Technology program in Applied Networking and System Administration.

Andrew is currently working for ITS in our Distributed Support Services (DSS) area. He is an Assistant PC Systems Administrator for the College of Engineering, working with Mark Chast. He also is responsible for system administration of the PCs in the NRH lab in the Residence halls.

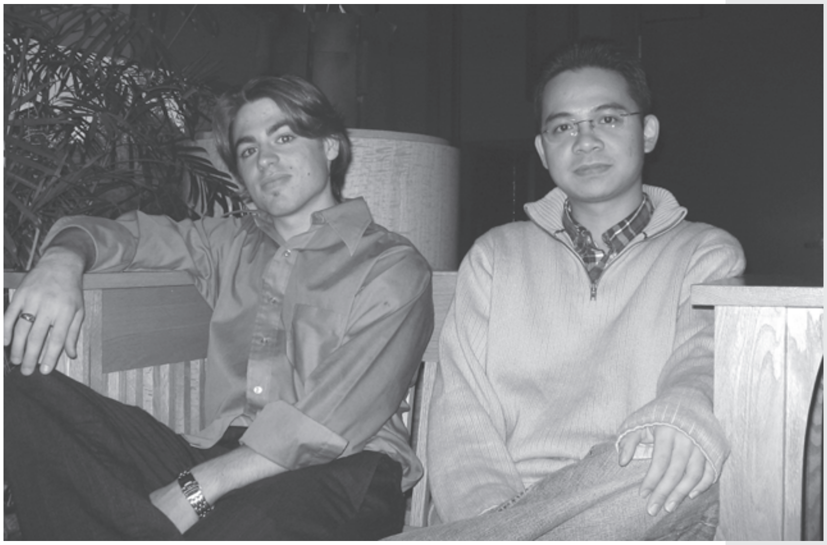
Continued on next page

He chose this particular co-op because he had worked for ITS in the Resnet area and liked the teamwork there. “It was a really great offer,” he said, and to also be able to work on campus was appealing.

Andrew loves music. In his spare time, he plays whatever instrument he can get his hands on. He also likes going to concerts, cooking, reading, working out, and running.

Of his job Andrew says, “ITS rocks my world.” He has met a lot of interesting and friendly people and enjoys the candy treats in the offices where he goes to assist people with their computers. He says that he has always been around computers and got used to fiddling around with them. However, when not working, he rarely touches computers, “unless I have to.” He prefers to involve himself in other activities.

We enjoy having Andrew on the team in ITS and look forward to working with him winter quarter.



Andrew Wurster and Minh Luong

Dianne Parker is part of the ITS Distributed Support Services team overseeing several co-op students and lab assistants. She coordinates the scheduling of some of the college computer lab facilities and supervises the ITS student employees within these areas. She can be reached at dianne.parker@rit.edu for questions related to computer lab facilities.

Sarah Haberbusch Celebrates 35 Years with ITS

By Debra Fitts

WOW! Sarah Haberbusch, Lead Operator, Technical Support Services Data Center Operations is celebrating her 35th anniversary of employment at RIT! We are so fortunate to have had her on the ITS staff since 1970!

In order to put the years into perspective, think about these facts:

- The top TV show in 1970 was Rowan and Martin's Laugh-In
- #1 song in April 1970 was ABC by the Jackson 5
- The Bestselling Album was *Bridge Over Troubled Water* by Simon & Garfunkel
- 1970 Academy Awards Best Picture: *Patton*
- Some items from 1970 Price Index include:
  - Gasoline $.36/gallon
  - Median Income $8,734/year
  - Median Rent $108/month
  - Bread $.24/loaf
  - First-Class Postage Stamp $.06
  - Harvard University Tuition $2,600/year

Well, enough of that…. Sarah started work at RIT on October 12, 1970 as a keypunch operator. At one time, there was a "keypunch" room in Data Center Operations with eight loud keypunch machines.

She performed data entry for all administrative systems on campus including Payroll, General Ledger, Student Records and Admissions. She also became the primary Data Control Assistant for the Payroll applications. This involved daily use of machines which sorted and collated thousands of keypunch cards.

As systems changed and applications developed, Sarah's role was critical for the input of data, batch update and printing for numerous customers. Her main focus was concentrated in the Payroll category while still maintaining knowledge of all the systems. After continual changes and the arrival of Oracle Applications, her position and responsibilities changed in major ways. She transitioned into the computer room as an operator.

Her current position has changed considerably from 1970, yet in some ways, still incorporates some of the same tasks such as printing payroll checks. She now plays an important role as Lead Operator for Data Center Operations.

We are so fortunate to have Sarah as part of our operations staff. Her experience in operations is invaluable as the department and her role continues to evolve. There are seldom ever two days alike in the Data Center!

Debra Fitts is Assistant Director, ITS Data Center Operations. She can be reached at debra.fitts@rit.edu

Desktop Support Analyst Cheryl Williams Celebrates 10 Years with ITS

By Vince Incardona

Years ago, there existed a popular myth which held that a person could start out in the mailroom of a large corporation, and eventually, through years of hard work, education and loyal service, rise to become CEO of that same corporation. Although most people would be hard pressed to name a real person that had done this, they nevertheless believed it to be a real possibility for themselves and their children.

Of course, nobody believes this anymore—economic trends in the last few years have effectively torpedoed that social contract, among others. Once in awhile, however, you run into an individual who makes you wonder what the possibilities are.

Such is the case with me as I reflect on Cheryl Williams' 10-year anniversary with ITS, and her twelfth with RIT. Cheryl started out with RIT in the spring of 1993 in a temporary assignment as a file clerk. Her job at that time was to move paper records in the Residence Life office from generic manila folders to a new set of folders with color-coded tabs. In the fall of that year, Cheryl began her academic career by enrolling in the Computer Science program in what was then the College of Applied Science and Technology. The following year, she decided to pursue a major in Information Technology.

Cheryl's first experience with what is now ITS was as a student employee at the HelpDesk in the Fall of 1995. Two months later, she was hired full-time on the extended and weekend shifts at the HelpDesk, and the following year, received her Bachelor of Science degree in Information Technology.

Cheryl continued at the HelpDesk after graduation, and in 1997, was promoted to Software Specialist. Her first assignment was on the campus-wide networking initiative that brought Ethernet to every room on campus. At the completion of that project, Cheryl continued as an ad-hoc software specialist during several divisional and departmental reorganizations.

Those reorganizations provided an opportunity for me to recruit Cheryl as a member of the newly-formed Desktop Support team, and having seen the no-nonsense way she could marshal resources to get a large, complicated job done, I jumped at that chance.

Cheryl's energy, enthusiasm and technical skill set the tone for the newly-formed student team in Desktop Support, and now, that drive and sense of purpose are an embedded part of our team's culture. As a software analyst, Cheryl not only has continued to lead ongoing efforts such as support of Project Lead-the-Way, but also does the critical day-to-day work of making sure our students are hired, scheduled to work, paid, and promoted on time. She has been an invaluable resource and an outstanding mentor.

While doing all of this, Cheryl has managed to find time to raise a daughter, who will turn 16 in January, earn a Master of Science Degree in Instructional Technology and a Certificate in Deaf Studies, become engaged, and together with her fiancé, begin building a house. She has come a long way since her start as a paper-based information specialist, and it has been inspiring to watch. Who knows where she'll be 10 years from now. CIO Williams? President Williams? Hey, you never know.

Vince Incardona is Team Lead, ITS Desktop Support, a part of the Customer Support Services Department. He and his staff work directly with customers in RIT Colleges and divisions troubleshooting various system and application issues. Vince was recognized in the previous issue of ITS News Magazine for his 20 years of service to ITS and is an inspiring story as well!

File Sharing Myths and Truths *Continued from page 9*

The Playing for the "Man" Myth

Heard in various formats, this myth goes something like, "RIT was sick of fighting this MP3 thing so they turned over a bunch of students to the RIAA."

Truth – The various agencies that want to protect the copyright holders in the music, movie, television, and software industries must take a legal action to subpoena the identity of an individual associated with an IP which is allegedly sharing copyrighted materials. RIT legal counsel reviews the subpoena. If the subpoena is considered legitimate, RIT is legally required to provide the information requested in the subpoena. The involved student is notified. Parents are notified if the student is a minor (again, under 21 years of age). Every attempt is made to give the student two weeks to consult with legal counsel. Only then, is the identity of the individuals named in the subpoena revealed to the agency.

The I Won't Get Caught Myth

Students have expressed this myth in a variety of formats from "my machine is too slow" to "my machine is only on a few hours a day" to "my music collection is so weird there is no one else interested so I just open it up so I can listen to tunes in the lab."

Truth – Among the people at RIT who have been cited for illegal file sharing are students with music they loaded while in middle school, students with obscure software, and students who only opened their share for the time they were in a lab.

The It Is Legal Because I Could Have Recorded It Myth

Students argue, "The show was on TV but I forgot to record it. So, I went out the next day and got it off the net. No big deal – TV shows are not copyrighted anyway!"

Truth – TV shows are covered by copyright. Getting copies of last night's *CSI* episode or the last season of *Friends* or any other show is a violation of copyright law unless you purchase a legal copy or have specific *written* permission from the copyright holder to have the copy.

The "All's Fair in Love and Academia" Myth

This is actually two myths. The "fair in love" refers to the argument that if you were only innocently or benevolently sharing copyrighted material, it isn't really piracy. The "academia" part is that all students and faculty (or staff) who work in academia are protected by the fair use provision of the copyright act. In other words, "If I am associated with academia, I am free to use copyrighted material in any manner I choose."

Truth – Ignorance of the law, ignorance of what your computer is sharing, and being a "nice" person are not protections from the sanctions associated with a law. If you are sharing or possess a copy of copyrighted work illegally, you are liable.

Fair Use refers to a provision in the U.S. Copyright Act that allows unauthorized, **limited** use of a copyrighted work in specific situations which are considered to be in the public good. This includes research, criticism, reporting of the news, and teaching. The T.E.A.C.H. act further limits use of copyrighted works. In general, a person associated with an educational institution as a student, faculty member or support staff member has very limited rights to use copyrighted materials and, in most cases, has no right to use a work *in its entirety without written permission from the copyright holder.*

The bottom-line is that pirating music, software, games, TV shows, and movies is illegal. You can argue the laws are antiquated, poorly written, misinterpreted or that you didn't know they applied. Each argument will carry little or no weight in a judicial hearing or in a court of law. You can risk your reputation, your money, your education, and your career on a felony conviction. Or you can understand the myths that are there and take corrective action to avoid the consequences.

Donna Cullen is the ITS Computer Policy Analyst. She works closely with RIT Judicial Affairs when RIT is presented with RIAA and MPAA subpoenas, presents educational programs about illegal file sharing at First Year Experience programs and is a member of the planning team for the ITS Security Week workshop series. Donna can be reached at donna.cullen@rit.edu for more information about the illegal file sharing issue.

Web Hosting Upgrade

By ITS Web Services Team

The Web Hosting Upgrade Project's goal is to provide RIT with a web environment that is secure, reliable, well maintained and responsive. The Institute's needs have outgrown the current web environment, and to meet the current and future needs of the Institute, a redesign of the entire environment is necessary. The project team has identified key steps that need to be accomplished to meet the goal of this initiative.

Major Steps

Separate Content. We need to separate official content such as college and admission sites from content like individual's web pages. This is to ensure that visitors to official RIT sites are actually at an official site. In the past, we have had issues where a student's class project for redesigning an official RIT website was mistaken for the official site. By separating content, we can avoid these issues. A side benefit of the separation of content is unusually high traffic to a student webpage that has popular images or information will not negatively affect official RIT sites.

Improve the User Experience. Improve the user experience for the audience of our websites by restructuring RIT sites into a hierarchy and removing the use of tilde (~) accounts. For example, the URL for the College of Science would be http://www.rit.edu/colleges/cos/. We also anticipate being able to provide multiple ways for College sites to be identified, including the following format: http://www.rit.edu/science/.

Eliminate the need for shared accounts for accessing and updating websites. To access websites, people will use their individual RIT Computer Accounts and will be assigned appropriate permissions for the sites they need to maintain.

Update the base web hosting technologies. We will be adding mySQL database hosting for the official RIT website and upgrading to PHP5. More information about the technical detail of the new web environment will be published shortly.

Plan for future upgrades. Working with the RIT Web Standards Committee and the RIT community, ITS will develop and publicize a planned upgrade schedule for the RIT web environment.

Create a staging environment for official RIT websites. Website maintainers would use this staging environment to make changes to the site and view the results before the changes are made public. Once the website maintainer is satisfied with the changes, they can push the new content into production using a set of web-based tools. These tools will help efficiently maintain the RIT websites. The project team is finalizing the design for the

Continued on page 30

RIT Hosted Explore Rochester IT Symposium

October 28 at GCCIS

RIT student Lindsay Simancek, shown at right with Deepak Seth, Manager and Americas Lead for Bausch & Lomb, was one of the first interns to participate in the Explore Rochester IT program this summer. She worked in the IT departments on a rotating basis at Wegmans, Paychex and RIT as part of a local effort to spotlight IT careers.

Lauren Bedugnis, a co-op student in ITS shows off the logo design for the Explore Rochester IT Symposium. She was instrumental in developing the concept for the "look" of the program as well as the web site where all information about the newly established program can be found. The Explore Rochester IT Symposium, attended by more than 200 students from area colleges, is an initiative of the CIO Roundtable to encourage IT graduates from local colleges to remain in Rochester after graduation.

Web Hosting Upgrade

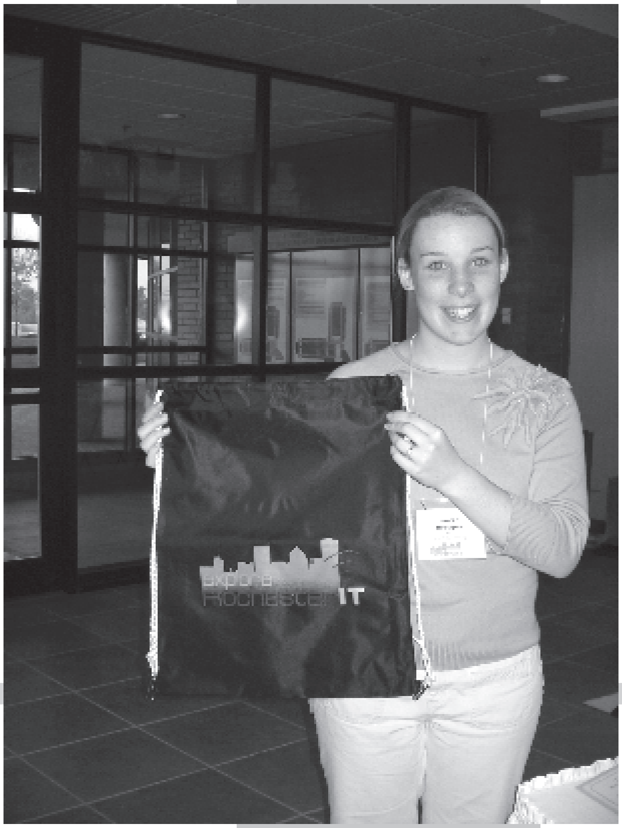
Continued from page 29

web hosting hierarchy and technologies. They will be presenting the web hosting hierarchy to the RIT Web Standards Committee for approval. Once the designs have been finalized, ITS will purchase the necessary equipment and begin creating the new environments. The new environments will undergo thorough testing, and when testing is complete, a pilot group of sites will be migrated to the new environment. After the pilot group of migrations has occurred and any concerns addressed, migrations for the rest of the official RIT sites will start. The project team has designed a way for the new environment and the old environment to exist seamlessly to the web audience so we can do a planned migration over a period of time instead of a single cut over to the new environment.

What does all of this mean to you?

If you maintain an official RIT website, the biggest change will be the restructuring of the web site hierarchy. In the new web environment, each college and division will have its own branch. From there the college or division determines the structure of the rest of their site within this branch. ITS will work with each area in setting up their structure during the migration period. If you have an individual web page under your personal RIT Computer Account, like http://www.rit.edu/~abc1234 or http://www.rit.edu/~abcits the biggest change will be the URL of your webpage. The proposed URL would look like http://persons.rit.edu/~abc1234.

Deepak Seth, Bausch & Lomb, with RIT student Lindsay Simancek



ITS co-op student, Lauren Bedugnis

Photos by M. Cometa, 2005

DSS Computing Labs

Hours, locations, hardware, software, and reservations information available at: http://www.rit.edu/its/services/computer_labs

Telecommunications Services

To contact Telecommunications Services call 475-5800.

ITS HelpDesk

Located in the Gannett building, rm. 7B-1113

To contact the ITS HelpDesk

- Call 475-HELP or 475-2810 (TTY)
- Send e-mail to helpdesk@rit.edu

Regular hours

Sunday	12 p.m.–6 p.m.
Monday–Thursday	7:30 a.m.–8 p.m.
Friday	7:30 a.m.–5 p.m.

ITS News is published quarterly for RIT students, faculty, and staff. It is available in electronic form at http://www.rit.edu/its

ITS News is created with AdobePageMaker 7.0 on a Dell OptiPlex GX260 and is printed at a service bureau through RIT's HUB. Photographs taken with Nikon COOLPIX 900 digital camera.

Managing Editor: Dave Pecora, dlpits@rit.edu
Editor: Michelle Cometa, macits@rit.edu
Design/Layout: Omar Phillips, odphelp@rit.edu
Editorial Team: Dave Bradstreet, Donna Cullen, Patrick Saeva, Alison Spath, John Whitely, Shawn Whiteside, Dave Hostetter (Team Oversight)

Use of registered trademarks does not constitute endorsement by RIT or ITS. Rather than put a trademark symbol in every occurrence of a trademark name, we state that we are using the names only in an editorial fashion, with no intention of infringement of the trademark.

ITS News is printed on recycled paper and is itself recyclable.

ITS Information & Technology Services

R·I·T