PLUGGED IN

Spring 2009: Volume 1 Issue 2

To Information Technology News @ The University of Rochester

In This Issue:

New University Policies

Protecting Social Security Numbers and Personal Identifying Information

The Data Security Task Force has been working tirelessly to raise awareness about the new University Policy on Social Security numbers (SSN) and Personal Identifying Information (PII) and the new Data Classification policy.

...continued on page #3

Think it Couldn't Happen to You? Think Again

A University employee shares the story of her own personal nightmare involving identity theft

At first, the letters looked like harmless junk mail. The first and last names of the man they were addressed to were so close to my own that I assumed they were bogus solicitations from marketing companies.

...continued on page #4

> My credit was frozen, my relationships strained, and my coping skills severely tested while I worked to undo the damage.

CIO Corner with David Lewis

Vice Provost & Chief Information Officer

This special edition of *Plugged In* is dedicated to security awareness. Here you will find a wide range of University-wide collaborative security measures — from our brand-new student and staff information security awareness campaigns to the "Security Tips of the Week" to the initiatives involving data encryption, new ID badges, and security assessment scans.

I felt it was important to devote an entire edition to this subject because as higher education institutions continue to adopt new technologies, threats to cyber security are increasing worldwide, and new compliance requirements will impact students, faculty, and staff. The need for individuals to protect themselves and University assets is growing.

The University takes information security seriously. It is well known that higher education and health care organizations are regular targets for hackers. Continuing to invest in information security best practices is critical in today's digital world and it is one of the University's top IT strategic planning priorities.

Provost and Executive Vice President Ralph Kuncl and Senior Vice President and General Counsel Sue Stewart co-chair a Data Security Task Force with leadership from across the University. Over the past year, the group has made great progress with information security policies that govern the use and storage of Social Security numbers and Personal Identifying Information. They have also developed new campaigns to promote the June 30 deadline for new SSN compliance and increase awareness of security issues.

While spam, viruses, and hoaxes continue to tax our email storage capacity and tie up IT support systems, security breaches not only interrupt operations and cost the University financially, they can also affect our reputation and alumni relations. Sophisticated criminals work hard every day to disrupt or destroy the security of our networks. We must be vigilant and continuous in our response. To successfully engage and support an institution as large and diverse as ours will require preparation, policy, persistence, and most of all, coordination of limited resources. Every one of us must take responsibility for better protecting our networks, equipment, and personal and business-related information.

I remain committed to finding new ways to bring effective security practices and increased security awareness to the University community. Thank you for your ongoing support and vigilance in this ongoing endeavor. I plan to keep you informed of emerging efforts so you can better "protect your computer, protect your data, protect yourself," and ultimately, protect the University as a whole.

Meliora,

http://www.rochester.edu/IT/cio/

New University Policies

Protecting Social Security Numbers and Personal Identifying Information

. . .cont. from page 1

The University Data Classification policy, which is incorporated into the existing IT Policy, Section III, addresses how long sensitive data needs to be retained, and how disposal of that data should be handled.

These policies went into effect in January and specify how we will protect Social Security numbers and employees' Personal Identifying Information. This includes employees' home addresses, home telephone numbers, as well as employees' SSNs and applies to any medium – paper, microfiche, electronic.

"The first protection step is to reduce the number of places we store these sensitive data, and being thoughtful about what we really need to retain," says Chip Nimick, Information Security Officer for the Medical Center and Data Security Task Force member.

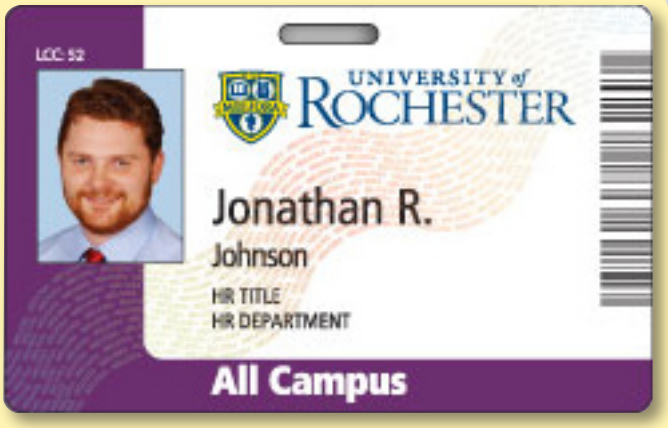
Also key is consolidating storage locations from individual office to departmental office to the University's Official Repository for that data (see link to Data Retention Policy below). On behalf of the Data Security Task Force, Nimick reminds everyone at the University, "as we dispose of unneeded copies of SSN and PII, we must do so in a manner that makes these data unreadable and unrecoverable. If we decide that we must retain a particular data collection containing SSN, we must register with a Privacy Officer of the University. "

This registration must be completed by June 30.

Details on the new University Data Classification policy can be found at:
http://www.rochester.edu/it/policy/

The Policy on Social Security numbers (SSN) and Personal Identifying Information (PII) and more information can be found at:
http://www.rochester.edu/it/policy/SSN-PII/

The Data Retention Policy is located at:
http://www.rochester.edu/adminfinance/records.html



The University is replacing ID badges for all faculty and staff. This project is designed to protect personal information, update photos, and enhance security by verifying access privileges to facilites and labs.

Employees will be required to get updated photos taken in the coming weeks. For a schedule of times and locations for badge replacement, or for more information, go to:
http://www.rochester.edu/working/hr/badges/

Rollout is expected to be completed by the end of June.

Julie Myers

Chief Information Security Officer

Have any questions surrounding security awareness? Chief Information Security Officer Julie Myers welcomes feedback from the University community. Contact her at 275-4363 or e-mail julie.myers@rochester.edu.

Click here http://www.rochester.edu/currents to read Julie's comments in a Currents article about the new information security policies.

Think it Couldn't Happen to You? Think Again

A University employee shares the story of her own personal nightmare involving identity theft

. . .cont. from page 1

The first signs of trouble came when I was denied a modest increase to my department store credit card. Then I was notified that I didn't qualify for a car loan I'd been certain I would get. And finally, the real red flag—a notice came informing me I was being sued for nonpayment of child support in Nassau County, Long Island.

I was single, living in Rochester, and didn't have any children when my seemingly simple life was turned upside down: Someone had stolen my identity along with my Social Security number. The clues that came in the mail were merely a hint at the destruction that followed. It was the beginning of a 10-year odyssey to clear my name, reclaim my identity, and restore my credit history, which I was just starting to establish.

I had to hire an attorney to help me navigate the maze of red tape I confronted dealing with the Social Security Administration, Child Welfare Services, and I.R.S. I was subpoenaed in order to testify to avoid having my wages garnished for a mountain of debts I did not owe. I had to take time off from work to sit for depositions and present evidence that I was the rightful owner of my Social Security number—and not the deadbeat dad who had skipped out on paying child support for his disabled daughter.

My credit was frozen, my relationships strained, and my coping skills severely tested while I worked to undo the damage.

I never was able to track down how my Social Security number was stolen, and it seemed like an unusual occurrence at the time. Unfortunately today, thieves are more sophisticated and more determined to rob ordinary citizens of their identities. They are online creating botnets, using phishing scams and malware. They may target your home by rifling through your trash, or even by stealing your purse or wallet while you're at work. They are always looking for vulnerabilities.

"Today, thieves ... may target your home by rifling through your trash, or even by stealing your purse or wallet while you're at work. They're always looking for vulnerabilities."

I know we can't expect 100% protection from identity theft, but I am encouraged to see that the University is enforcing new policies regarding Social Security numbers and other personal information. We all must be vigilant to help safeguard patients', students' and staff and faculty members' private information. I don't want the nightmare that I endured to happen to anyone else.

Colleague Spotlight: Peter Chesterton

Chief Privacy Officer and Chief HIPAA Security Official - UR Medical Center

Peter Chesterton has been Chief Privacy Officer and Chief HIPAA Security Official for the University of Rochester, Medical Center since 2003. He is also Senior Director for Resource Analysis and Management at URMC and serves on several committees, including the HIPAA Steering Committee and the Data Security Task Force. Chesterton, who holds an MBA from Rochester Institute of Technology, began his career at the University in 1971. His previous positions in the School of Medicine and Dentistry include Associate Dean for Administrative and Fiscal Affairs, Director of Finance and Departmental Administrator, and Budget Officer for the University.

PI: What do you value in your colleagues in information technology?

I value the planning, technical, and support skills of my colleagues in information technology. Providing information technology infrastructure and services in support of the University's education, research, patient care, and community service missions is a tremendous challenge. To meet that challenge, while at the same time providing a secure physical and technical environment, requires a team effort. I value being part of the team charged with that responsibility.

PI: What are some of the challenges you face with IT that are unique to your work at the Medical Center?

Information technology offers us some extremely valuable and powerful tools with which we can quickly provide accurate information to educators, care providers, researchers, and administrators. Much of that information is individually identifiable and confidential. One of the biggest challenges we face at the Medical Center is keeping pace with the capabilities the technology affords us while at the same time maintaining and improving the security and privacy of the information entrusted to us.

"One of the biggest challenges we face is ... keeping pace with the capabilities the technology affords us while ... maintaining and improving security and policy."

PI: If you could change one thing about IT at the University, what would it be? Or, what would you like to see?

One fairly recent change has been the establishment of the UR Data Security Task Force. The Task Force has identified and addressed some significant data security issues ... and provided a forum for discussion, information sharing, and priority setting. It has been a very positive change in the way we address information security. New issues are constantly emerging, so I would like to see a continuation of this type of interaction.

PI: Of everything IT provides, what enables you to be successful; something you can't live without?

Certainly ... email, the use of web-based applications, and portable devices, such as laptops would be difficult to live without. We can't live without the IT facilities and technical support staff that keep those services available.

PI: Can you cite some past success you've had with IT or highlight some current/future projects you're excited about?

In the Medical Center, we've

...continued on page 6

Top Ten IT Issues for 2008

Which IT issue is of top concern to technology leaders in higher education today?

The ninth annual EDUCAUSE Current Issues Survey has the answers.

1. **Security**
2. **Administrative / ERP / Information Systems**
3. **Funding IT**
4. **Infrastructure**
5. **Identity / Access Management**
6. **Disaster Recovery / Business Continuity**
7. **Governance, Organization, and Leadership**
8. **Change Management**
9. **E-Learning / Distributed Teaching and Learning**
10. **Staffing / HR Management / Training**

Survey participants, typically CIOs of EDUCAUSE member institutions, were asked to check up to five issues in each of four areas: issues that are critical for strategic success, issues that are expected to increase in significance, issues that demand the greatest amount of the campus IT leader's time, and issues that require the largest expenditures of human and fiscal resources.

EDUCAUSE is a nonprofit association whose mission is to advance higher education by promoting the intelligent use of technology. EDUCAUSE helps those who lead, manage, and use information resources to help shape strategic decisions at every level.

. . .cont. from page 5

recently completed installation of full disk encryption software on all of the centrally managed laptop and desktop computers. This has provided a significant increase in the security of information stored on those devices. We continue to work on installing the software on locally managed devices.

Providing privacy and security education of faculty, staff, students, and volunteers is an ongoing challenge. During 2009, we will be incorporating locally written and produced training videos as part of our required training. They will be available online as part of new hire orientation. Also, *HIPAA Highlights*, a monthly electronic newsletter, continues to be an excellent way to keep up-to-date on our privacy and security requirements.

Implementing the SSN and Personal Identifying Information policy is an extremely important project that extends well beyond the University and Medical Center IT departments. Everyone has a responsibility to protect sensitive information (see cover story).

PI: What future IT opportunities are you looking forward to?

Believe it or not, the "Stimulus Package" -- American Recovery and Reinvestment Act (ARRA) -- actually has some significant privacy and security components that will require our attention in the immediate future. As part of ARRA, the Health Information Technology for Economic and Clinical Health Act (HITECH) provides for $19 billion over a four year period. Grants and loans are to be provided for infrastructure and incentive payments under Medicare and Medicaid to providers who adopt and use health information technology. Privacy and security provisions are being expanded under HITECH, which will require us to reexamine and update our policies and procedures.

PI: Where else do you see IT growth or changes?

Increased use of electronic health records and the exchange of information in those records is certainly a national and regional priority. The Rochester region, like many other communities in New York and across the nation, is developing a regional health information organization (RHIO). The RHIO is an electronic network of patient medical information gathered from area providers and hospitals. With the patient's permission, providers can view lab reports, test results, medication history, and other information, regardless of where the patient may have been seen. The goal of the RHIO is to improve care by having more complete information immediately available to providers when they are treating patients. Having this information should reduce inefficiencies and lower cost through fewer duplicative tests. Maintaining the privacy and security of that information is an essential ingredient to making the RHIO a success.

Protecting University Assets through Encryption

Protecting Your Data in Case of Theft

The University has a legal obligation to protect an individual's Social Security number (SSN) and Personal Identifiable Information (PII). Data encryption is one of the ways in which the University ensures this protection.

Desktops, laptops, and mobile devices (such as Blackberries) have the capability of storing SSN and PII data. Encryption transforms data on these devices from a readable state to an encoded state to protect the data. This is especially important if these devices are lost or stolen.

Encryption allows us to accomplish two goals: it protects an individual's private data and it protects the University's reputation.

Where are we now?

The University has encrypted 15,600 high-risk desktop computers, approximately 14,200 of these in the Medical Center. These devices were known to possess SSN and PII data. We are currently scheduling additional desktops for encryption. Beginning in 2009, the University also started encrypting Blackberry mobile devices.

What are we doing?

The University has launched a Security Awareness Campaign, to increase awareness of this important issue (see article on Page 8). Protecting data is one of the cornerstones of this campaign and individuals are encouraged to consider data encryption, especially if they have sensitive data on any of their electronic devices.

What should you do?

The best thing to do is to remove SSN and PII data from your electronic devices. If you have questions or would like to request encryption for your electronic devices, contact your Privacy Officer.

Privacy Officers:
Non Medical Center 273-1804
Medical Center 275-7059

Spam Hits a Speed Bump

Solution Softens the Blow of Incoming Spam

Slowly but surely, the days that begin with an email inbox flooded with spam are dwindling. Since Sophos PureMessage was implemented in the fall of 2007, statistics show that spam has reduced from a daily maddening onslaught to an occasional minor annoyance:

In November 2008 *(see fig. 1)*, a new policy was implemented that discards messages scoring a 98%+ spam score. Think of the additional storage we are saving!

Although you may still occasionally receive an email that is spam, recent efforts have contributed significantly to the leanness of your inbox.

Fig.1 Messages marked as spam over the past 6 months:

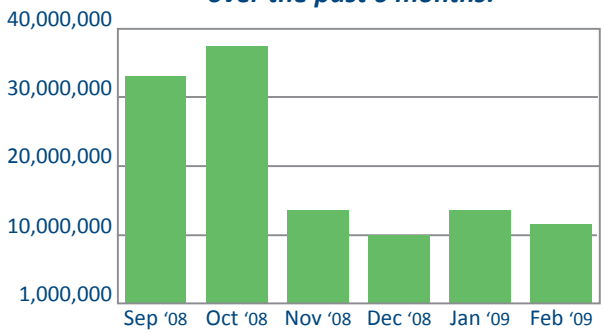
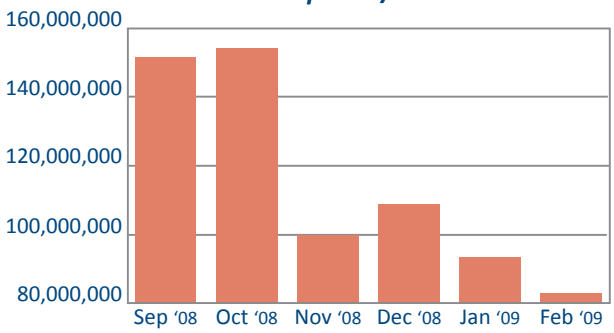


Fig. 2 Connections that were dropped before they even reached our servers based upon IP/hostname:



These graphs represent non-Medical Center statistics only. The Medical Center is seeing similar results in Spam control from their Spam management system.

A Fresh Look at Security Awareness

Educating the University of Rochester About Cyber Safety

"Protect Your Computer. Protect Your Data. Protect Yourself." This tag line, which appears on many of the campaign materials, represents the overarching goal of both our student and faculty/staff security awareness campaigns.

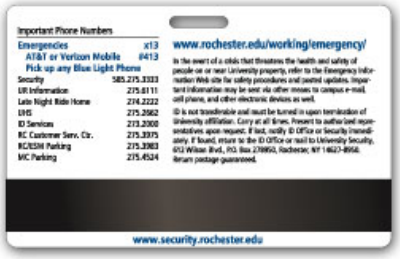
Have you seen the flyers and posters around campus? This non-traditional approach was used to grab attention and help students learn about information security threats and how they might better protect themselves. In addition to these posters and flyers, students could attend a tabling session or take advantage of the "Security Tip of the Week" in *Weekly Buzz*. To measure the effectiveness of this campaign, an online survey was given to students with a prize giveaway of a Nintendo Wii from University IT Computer Sales. 655 students completed the survey, which ran March 16-27. Results from the survey will be used to refine this campaign for 2009-10.

Unlike the student campaign, the security awareness campaign for faculty and staff is primarily focused on the proper use and storage of protected and confidential information. Recent policies include a Social Security number (SSN)/Personal Identifying Information (PII) policy (see related cover story), a Data Retention policy, and a Data Classification policy. Compliance is being encouraged by the President of the University. Information Security and Privacy Officers attend department meetings to discuss how each department can better comply with these new policies. A Security Interest Group (SIG) has also been formed with participants from several departments across the University community. In addition, weekly security tips geared towards faculty and staff ran in *@Rochester.*

Do you know how to contact UR Security?

The Answer May Be Easier Than You Thought

Do you know how to contact UR Security? Who to call in the event of an emergency? Report a crime, parking lot incident, or strange occurrence? Look to the back of your ID badge!



Or, for non-emergencies, contact University Operators by dialing "0" from any University phone, or 275-2121 or 275-2100 from any non-University external phone

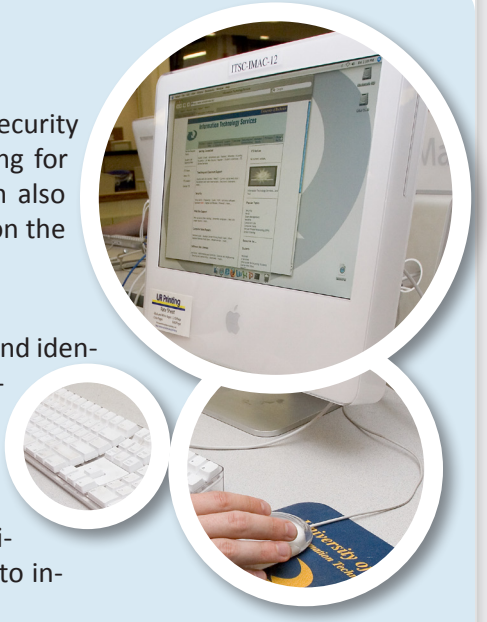
For more information, go to: http://www.security.rochester.edu/safe.html
Questions or concerns? Call x5-2000.

Information security officers hosted three question-and-answer "tabling sessions" in Wilson Commons; door hangers and flyers were handed out to improve the retention and recall of these important messages.

By using edgy graphic elements and creative wording, Information Security made effective marketing tools that captured the attention of students.

Security Assessment Scans

Evaluating Applications and Devices



Security assessments provide a way for system administrators to evaluate the security of the systems they manage. Assessment information is obtained by scanning for security issues on network-attached devices and open ports. Information can also be gathered by running services for applications and operating systems in use on the University network.

System administrators then utilize the results to evaluate the system's security and identify remediation tasks needed to bring the system into compliance with University standards.

The University IT Security and Policy Office can perform an assessment for department systems upon request. Scan requests will be evaluated based on criticality of application and availability of resources. Future scans will be offered to include content based inspection of file servers and web-based applications.

To ensure the security of a system, the University IT Security and Policy Office recommends scans at the following times:

- Each stage of the Server Implementation Lifecycle
- Operating System Installation
- Application Installation
- Database Installation
- Move to production (go-live)
- Any upgrades or significant modifications to the above items

Why should you have a security assessment performed on a system you manage?

- As software and operating systems age, the number of vulnerabilities for them increases.
- Attacks against web application vulnerabilities are quickly changing in complexity and in their ease of use.
- Open environments lend themselves well to more targeted attacks from outside intruders.
- By identifying vulnerabilities that exist in a system, actions can be taken to reduce exposure to malicious attacks.
- Information provided in an assessment can help educate system owners and administrators on how to develop and utilize best practices for securing system configurations.

To schedule an assessment scan of your systems, please contact the IT Center at 275-2000 or via email request to UnivITHelp@rochester.edu. Requests will be performed as priority and scheduling permits.

Is *Plugged In* Meeting Your Needs?

Send feedback, article suggestions, and submissions to:

Managing Editor: Samantha Singhal - Samantha.Singhal@rochester.edu - x 32607
Design & Layout: Kelly Ernst - Kelly.Ernst@rochester.edu - x 63872
Editor: Mercedes Fredericksen - Mercedes.Fredericksen@rochester.edu - x 63873