

New RIT University ID to Replace Social Security Number for Safer Campus Identification

by Dave Pecora, ITS Customer Support Services, Dave.Pecora@rit.edu

RIT has undertaken a major project this year to replace Social Security Number as the primary identifier of students, faculty, and staff. Social Security Numbers will still be stored by the University and used where needed by law, but its use as a means of general identification on campus will end this May.

RIT will create a new number for identification purposes – the RIT University ID. This new number will replace the Social Security Number as the most commonly used unique identifying number for transactions done on campus.

New ID cards will be issued to everyone, starting with faculty, staff, and those students taking classes in the summer quarter. ID cards will be preprinted using existing photos on file – no one will need to get a new photo taken. For faculty, staff, and those students taking classes in the summer quarter, new ID cards will be available for pickup at the Registrar's office in May. Students returning in the fall that are living in on campus housing will receive their new ID cards from Housing Operations as part of fall move-in.

Two early community forums about the project will be offered by ITS in February:

Thursday, February 23

1-2:30 pm

The CIAS Auditorium (76-1125)

Friday, February 24

11 am -12:30 pm

The CIAS Auditorium (76-1125)

These forums are general information sessions on the project, the timetable for conversion, the process for picking up the ID card, as well as an opportunity to answer any questions about the process. They will be open to all members of the RIT community. Other forums will take place throughout the Spring Quarter.

Faculty/Staff Replacement Card Pick Up Process

Faculty and staff will be advised about their replacement cards and the timetable for picking

them up at the Registrar's Office. Tentatively, the new ID cards will be printed in April for distribution at the Registrar's Office after May 1st.

The project is being managed by a campus-wide team, with representatives from all colleges and divisions. More information about the project – including a list of project team representatives by college and division – can be found at <http://www.rit.edu/its/initiatives/sirp/index.html>.

New SPAM-filtering Solution Implemented

With the new SPAM-filtering solution, *mySpam*, operational, email users should see a noticeable reduction in the amount of SPAM in their inboxes. The mySpam solution will filter nearly all known variations of SPAM at the RIT mail gateway AND at users' desktops.

The RIT mySpam solution is based on the Brightmail anti-SPAM appliance from Internet security leader Symantec.

It works in three steps to filter messages:

- It identifies legitimate email and sends it to your inbox.
- It filters out all the known bad messages containing SPAM, viruses, phishing scams, etc.
- It develops a daily report of the messages it quarantined and sends this to users.

Identifying Legitimate Email and Filtering SPAM

Millions of emails come into the RIT gateway in any given month; nearly 10 percent of them being legitimate messages, said Tom Dixon at a mySPAM training and demonstration in December. The remainder is considered SPAM. In the past, ITS kept abreast of the inundation of nuisance email looking to resources such as known SPAM senders and alert messages from SPAM @ rit.edu. This information was manually inputted to a SPAM filter list at the network level.

mySPAM continues the filtering process. The software tags known SPAM before it gets to the mail servers on campus. "The system offers real time updates of known SPAM," said Dixon. Every 5-7 minutes the software receives information about identified SPAM and where these messages originate. This automated process frees up staff to address the few 'new' SPAM messages that creative spammers send, usually from infected computers.

What Users See: Reports and the Quarantine Process

Each day, any SPAM that happens to get through will be put into quarantine. "The system recognizes that these few messages may be SPAM," said Dixon. At this point, the messages are put into a separate area on the server – not directly in a user's mailbox. Users will receive a daily report about what is in this quarantine area. **These reports will have the subject line "RIT Spam Summary (Quarantined email)" sent from spamreport@rit.edu.**

The daily reports will allow users to see the list of messages quarantined. It will allow you to review the list, delete all the messages and release ones considered legitimate mail. You may also leave messages alone, and the system itself will automatically delete all quarantined items after 14 days.

Some additional mySPAM features:

- The new software has a low risk of false positives
- There will be no delay in delivery time of email messages
- The software has both Anti-virus and Anti-spyware facets to greatly reduce the chances of viruses entering the RIT system
- With this product and the filtering capabilities, spammers will be unable to “harvest” email addresses (this is the process spammers use to try all variations of an email address at a single domain, noting which are legitimate and which messages come back to them ‘undeliverable.’)
- Zip files, previously removed as a network security prevention measure, can now be sent and attachments up to 20 MB also can be accommodated

In the pilot for the new filtering system, users asked if email from list servers or other business-related services would be considered SPAM. It will not remove mail from generated lists, such as companies that you have done business with in the past and/or have provided your email address.

Those using a PDA, such as a Blackberry device, or Outlook Web Access (myMail) also will be protected with mySPAM. Its protections begin at the mail gateway and when users connect remotely, the filtering application will have removed the majority of SPAM messages that might have been listed in the Inbox area.

Any SPAM that might get through to users’ Inboxes can still send the information to SPAM@rit.edu. By doing this, the list of known SPAM will be increased and added to the filtering application.

If you have any questions regarding mySPAM, contact the ITS HelpDesk at 5-4357 (HELP), 5-2810 TTY or helpdesk@rit.edu

Or, for more information on how the reports and user interface works please visit:

<http://www.rit.edu/its/services/email/spamfilter.html>

Kimble's Corner:

Unwired Access Comes with Some Strings Attached

by Mark Kimble, Communications Engineer III, Mark.Kimble@rit.edu

During the 10th week of classes of the Fall Academic Quarter the ITS HelpDesk received several calls from users of the RIT wireless network in the Student Alumni Union (SAU). Their complaint was, they keep getting dropped from the wireless network.

An evaluation of the wireless access points providing WiFi service to the SAU found nothing wrong with the wireless infrastructure. There were users connected to the wireless network, and it was passing traffic. Yet, ITS continued to receive complaints about dropped wireless connections in the building.

After several trips to the SAU with laptops and WiFi analysis tools we discovered the culprit: cordless telephones. Why do you ask? Because the phones and the WiFi gear both operate within the same band of frequencies.

Ok time for a quick review/introduction of the underlying technology of WiFi and similar devices. (This could get a little geeky, but I'll do my best to stave off the wrath of the ITS Magazine Editorial staff.)

To the great chagrin of cable and wire manufactures everywhere, everyone wants everything wireless. We have cordless phones, wireless laptop computers, wireless keyboards and mice, wireless headsets (for your otherwise wired phones,) wireless baby monitors with built in video, wireless web cams, you name it. You name the technology and we the consumers want it wireless.

The problem with this is the radio frequency (RF) spectrum in which the manufacturers and you the consumer are allowed by the FCC to operate all of this disparate equipment within fits into a few very small bands of the whole RF spectrum. Typically all of these devices operate near 900MHz, 2.4 GHz or 5.4GHz as outlined in the FCC's Part 15 of Title 47, Code of Federal Regulations (CFR). (And you want *me* to keep it simple!)

Now as this is an institute of higher education I feel it is within my charter to assert some analogies from other disciplines and experiences. With the possible exception of somewhere within the Swartzchild radius about a black hole (a place I've never been to substantiate this), two objects cannot occupy anything close to the same space at the same time. Don't believe me? Try to watch TV with a hyperactive five-year-old and jealous two-year-old vying for your lap space (also known as your exact path of vision to the TV).

But I digress. The same sort of problem exists within the RF spectrum. Two devices operating within the same frequency spectrum will interfere with each other degrading, if not destroying, the performance and capabilities of each other. This is bad for you the wireless consumer and the perceived customer service expectation of the ITS supported RIT wireless network. Bad.

To date, ITS has deployed upwards of two hundred access points across campus at the request (and funding) of our customers. These access points are generally IEEE 802.11b gear all operating on the 2.4GHz band with careful selection of channels within that band to ensure best coverage of the targeted wireless hot zones with minimal interference from each other. Cordless phones, Bluetooth devices and wireless what-have-you are also widely deployed ad-hoc in the

2.4GHz range as well and they don't play very nice together. One phone call on a cordless phone can disrupt the wireless connections of any users within hundreds of feet of the phone.

ITS Communication Services has the tools and knowledge to engineer, deploy and support a wireless infrastructure that will meet the needs of the RIT community. In an effort to maximize infrastructure performance and availability, we will happily assist you in evaluating, specifying and installing any wireless technology you need to accomplish your mission; please feel free to call us.

So please:

1. If you need wireless network access for your department or area please go through ITS. We will assist you by designing, configuring, purchasing, installing and supporting your wireless network.
2. If you need a cordless phone please call us to evaluate and specify the best solution for your area and processes.
3. If you experience problems with your connection to the ITS-supported wireless network, please call the ITS Help Desk at 5-HELP. Tell them your situation and we'll do our best to isolate and remedy the situation using the specialized tools and knowledge we have for wireless networks.

This is a hostile RF environment we operate in. Even microwave ovens operate near the 2.4GHz RF range and can disrupt wireless connectivity on campus. As we continue to develop our WiFi network and add new services such as Voice over IP (VoIP) on the wireless network your cooperation will be very much appreciated by everyone using this shared RF space.

Check Closings with Campus Cancellations Hotline

With winter here, campus closings are a strong possibility. To ensure that our students, faculty and staff know of closings, an automated call line provides information about cancelled day, evening and weekend classes or special events due to weather conditions or other emergencies. To access this line, dial:

475-7075 (voice)

475-7076 (TTY)

Please share this information with your co-workers and student workers. It may save them a trip to campus while we are in the throes of one of our infamous Rochester snow storms!