

In Touch

Vol. 15 No. 2

Winter 2008

ISSN 1198-8673

In this issue:

NSC237 — Lights Out!	1
New Google Search Engine	3
Telecommunications News - VoIP Telephony	3
10 Threats to Computer Systems ...	4
Story with a Happy Ending	6
Getting Started in Second Life	7
Upgrading the Outlook Connector	8
Lights Out Photos	9-10

NSC237 — Lights Out!

Doug Vandevrie <dougv@uwo.ca>

Friday, 12 December, 2008 brought to a close a long era of service for NSC237 - Western's former primary Machine Room. About sixty current and former ITS staff members gathered for a celebration and refreshments in the NSC Machine Room. Many good memories and laughs were shared as people watched a slideshow of historical pictures, and comments on times past, technology changes and challenges faced were heard all around.

Jeff Grieve, ITS Associate Director, Technical Support, described many humorous moments in his commentary about the move and events over the previous months. He thanked all those involved in the project over more than two years and praised the

work done to make the entire move appear effortless and seamless.

Shortly after 3:00pm, Denis Regnier, former Associate Director, Technical Support, officially shutdown the last remaining server in the facility and Jeff Grieve (doing a little "hands on work") officially turned off the last remaining A/C.

A "signature" wall was in place to record those in attendance. This memento now hangs in the Technical Support area in the Support Services Building.

Thank you to all involved in making the move and this event a success. We look forward to a whole new set of memories in Western's new Data Centre.

More photos on pages 9 and 10.



Scheduled System Maintenance

**Sundays
6:00am - 12:00 noon**

Need help, have a question?

- Call the ITS Customer Support Centre
519 661-3800 ext.83800
- ASK ITS at <http://askits.uwo.ca/>
- Email using the Web Form at
<http://www.uwo.ca/its/helpdesk/question.html>

About *In Touch*:

Published quarterly by
Information Technology Services,
The University of Western Ontario.

Editor: Merran Neville

Printed by Graphic Services,
The University of Western Ontario.

The purpose of *In Touch* is to inform
our users about activities and events
of Information Technology Services.

Copyright ©2008 The University of
Western Ontario. Permission is
granted to copy in whole or in part
provided that due credit is given to
the author(s), the Division of
Information Technology Services,
and The University of Western
Ontario.

We welcome your comments,
suggestions, and articles.

The Editor, *In Touch*,
Information Technology Services,
Support Services Building,
The University of Western Ontario,
London, Ontario, N6A 5K7

Phone: 519 661-2151
FAX: 519 661-3486
Email: in.touch@uwo.ca
WWW: <http://www.uwo.ca/its/>



ITS Mission

We are committed to
delivering the best information
technology services and solutions
in support of the teaching and
research missions of the
University.

ITS Vision

To be recognized as the
preferred source of information
technology services and solutions
within the campus community
and recognized as one of the
leaders in the North American
university community.

Network Backup Service

For network backup and
recovery service please contact
the ITS Legato Group, e-mail:
legato@uwo.ca For details see:
[http://www.uwo.ca/its/network/
backup.html](http://www.uwo.ca/its/network/backup.html)

ITS OPEN HOURS

Building hours and hours of
opening for the various areas of
ITS are listed on the web at
[http://www.uwo.ca/its/reach/
contactus.html#hours](http://www.uwo.ca/its/reach/contactus.html#hours)

In Touch Mailing List

Additions, deletions, and
changes to the mailing list can be
made using the form on the web
at [http://www.uwo.ca/its/doc/
newsletters/InTouch/
subscription.html](http://www.uwo.ca/its/doc/newsletters/InTouch/subscription.html)

ITS Services 2008-2009

<http://www.uwo.ca/its/services.pdf>

New Google Search Engine

Kim Hoffman <khoffman@uwo.ca> and Judy Steward <judy@uwo.ca>

Search:

Since Google is the search engine of choice for 80 percent of Canadians and 69 percent of the worldwide web, ITS has recently chosen to also adopt this industry standard. When the license for the Autonomy Ultraseek search engine expired in December 2008, we purchased a two year license for a Google Search Appliance. This license allows us to index up to 500,000 documents. Sites that are indexed can be found at <http://www.uwo.ca/official.html>

The Google search engine allows both searching within a departmental site and across various selected sites as well. An example of a search restricted to a department can be found at the web site for the **Office of the Ombudsperson**, <http://www.uwo.ca/ombuds/>. The search box at this site will only search the web pages for this department, in other words, only pages that start with <http://www.uwo.ca/ombuds>. To customize your search box to your department, please read the document *How do I ... use the Western Search Engine* found at <http://www.uwo.ca/its/doc/hdi/web/search.html#restrict>

Google also offers the ability to create multiple collections. However, there is a 'performance' limit to the

number of collections that can be created. We are currently offering to create collections for faculties and top-level administrative units which have web sites spanning multiple domains. For example, a faculty search could limit the search to all the departments for that faculty.

If you want to set up a collection for your faculty/budget unit or have further questions, please contact its-search@uwo.ca.

An article covering the acquisition of the Google search engine appeared in **Western News** in December. The link to the article is http://communications.uwo.ca/com/western_news/stories/google_contracted_as_web_search_engine_20081219443425/

Telecommunications News -- VoIP Telephony

Mona Brennan -Coles <mona@uwo.ca>



Following the completion of the deployment of VoIP to the Support Services Building, the deployment to the rest of campus began recently with the Robarts Research Institute (RRI) move to Western's VoIP service the weekend of January 31.

The main Robarts number 519-663-5777, fax number 519-663-3789, and the Robarts Clinical Trials number 519-663-5700 remain the same. Other Robarts numbers have been changed and are listed in the Western Directory <http://www.uwo.ca/westerndir/>.

The Material Sciences Addition and the new sports facility (TRAC) have also been converted to VoIP. Seibens Drake Research Institute, West Valley Building, Avian Research and ICFAR building are the next buildings to be converted to VoIP.

We are continuing to prepare buildings for the conversion to VoIP. Other buildings in progress are Dental

Sciences, Medical Sciences, Health Science Addition, Kresge, Molecular Biology, Clinical Skills, Taylor Library, Chemistry, Biological & Geological Sciences Phase II.

Details about the **Campus Phone Systems** are online at the ITS web site at <http://www.uwo.ca/its/campusPhoneSystems.html>

Top 10 Threats to Computer Systems Include Professors and Students

Jeffrey R. Young

Copyright 2009, The Chronicle of Higher Education. Reprinted with permission.

From the December 19, 2008 issue of The Chronicle of Higher Education. <http://chronicle.com/free/v55/i17/17a00901.htm>

Karen McDowell spent several days this fall dressed in a purple fish costume, holding a plastic spear.

Ms. McDowell, a network-security analyst at the University of Virginia, wanted to raise awareness about “phishing,” e-mail schemes in which con artists send messages to trick people into giving out passwords or other personal information. Ms. McDowell walked around high-traffic areas of the campus to get attention. “Sometimes I introduced myself as a fraudulent e-mail because many people don’t know what a phish is,” she said.

The outfit hooked curious students, who asked her what she was up to, and most listened to her spiel. In the past, plainclothes administrators set up tables and handed out brochures about the importance of computer security. But Ms. McDowell felt that such efforts made little impact, since students mostly walked by without stopping. The fish costume was her idea — the university paid a local seamstress \$60 to make it — because she felt that a bit of flashiness and humor would help the message sink in.

User awareness is growing in importance when it comes to computer security. Not long ago, keeping college networks safe from cyber attackers mainly involved making sure computers around campus had the latest software patches. New computer worms or viruses would pop up, taking advantage of some digital hole in the Windows operating system or in

popular Web software, and officials would work to plug the gaps.

Those were the good old days — back when many big attacks were started by hobbyists who got a cheap thrill watching geek squads scramble.

Today a growing number of network bad guys are professional criminals, and they’re looking to steal real money. They don’t just want to post an embarrassing note on your college’s home page. They want to nab the identities of students and professors to go on shopping sprees with forged credit cards. With the global economy getting lousier, officials predict that even more hackers will get into the act in search of easy cash.

Increasingly, the weakest part of a network is the users, who carelessly give out their passwords or leave important information for the taking.

That’s the confusion I reached at a recent Dartmouth College conference on “Securing the eCampus: Building a Culture of Information Security in an Academic Institution” where I was asked to give my take on security threats. I compiled the following top-10 list of campus computer-security risks based on several recent computing surveys and interviews with more than a dozen college-technology leaders. The list, ordered from least to most serious, is by no means scientific, but it gives a sense of where today’s battle lines are — and why “phish” costumes should become more common on campuses.

Threat #10: Spammers

The unwanted e-mail advertising messages named after canned meat represent a constant attack on the campus, and collectively they can have a significant impact on network performance. Even though many

colleges can stop most spam messages before they reach users, filtering out ads for Viagra diverts energy away from other activities that IT officials could be doing.

More important, spam is an underlying factor in other network-security problems, since some attackers aim at college networks to help them send more spam, by hijacking student computers and turning them into spam servers. So if spammers could be stopped, that would help reduce other kinds of network threats.

Threat #9: Cellphones

The number of iPhones and other Web-surfing smartphones on campuses is growing rapidly. Since some phones can connect to wireless networks that blanket campuses, it is easy for students, professors, and administrators to do all sorts of communication on their phones that they used to do on their laptops. Which is great, until hackers create viruses for cellphones or until a user loses a phone with sensitive data stored on it. And so far, smartphones are harder to secure than laptops or desktops because virus-detection software can quickly run down cellphones’ batteries.

Threat #8: Phishers

Phishing scams are getting more sophisticated. Some early e-mail messages that attempted to trick users into revealing passwords were littered with spelling errors or poor grammar, tipping people off that they were fakes. But today the bait is more lifelike.

In a scheme that has emerged in the past year, scammers pretend to be college network officials asking recipients for their network ID’s and passwords. Colleges are struggling to

educate students and professors that they should never, ever give out their passwords via e-mail.

Threat #7: Social Networks

The popular Facebook social-networking system was invented by a college student, and students are among its most enthusiastic users. But cybercriminals have found that social networks are ideal pools for phishing attacks.

A study by Indiana University researchers showed that phishing schemes were much more likely to trick people on social networks than via e-mail — in some cases getting 70 percent of users to fall for the scam. In one popular scheme, students get a message that appears to come from a friend, saying that if they click a link they will see a video clip that they appear in. The link takes users to a site that tries to install malicious software on their computers.

Threat #6: Outsource Partners

Colleges are outsourcing more technology services than ever these days, putting the security of campus information in someone else's hands. Calling vendors a "threat" is probably too strong, but companies can be a point of vulnerability for campuses. Case in point: This April a contractor for SunGard Higher Education had a laptop stolen, and it contained data from 18 colleges that were clients of the company. For one of those institutions alone, Connecticut State University, the laptop had data for 3,502 students and alumni from four campuses.

Threat #5: Students

Every year students seem to become more careless about computer security, according to some college officials. Students will happily give their passwords to friends to check

their e-mail for them. Or they'll create simple passwords that are easy for attackers to guess.

Threat #4: Professors

The only people more careless on their computers than students are professors. When a phishing scheme hit Stanford University this year, for instance, the vast majority of those who fell for the con were faculty members.

Threat #3: Staff Members

Some colleges collect more sensitive information than they need, leaving more opportunities for the data to be exposed to the public or swiped by hackers. Several recent reports said mistakes by careless employees had caused more data breaches than outside attackers had.

Threat #2: Thieves

Thefts of computers with sensitive data have increased each year for the past five years, according to the latest survey by the Campus Computing Project, which tracks college IT trends. This year more than 30 colleges have reported lost or stolen computers or hard drives with sensitive data on them. As laptops get smaller and flash drives get more capacious, this threat will very likely grow. Officials recommend that professors and administrators encrypt sensitive data so that criminals won't be able to see such information on laptops they've swiped.

Threat #1: Malware and Botnets

The Georgia Tech Information Security Centre estimates that 15 percent of online computers worldwide are part of botnets: millions of computers infected with malicious code that lets attackers turn them into "zombies" for their own evil electronic deeds (botnets are often used to send spam). That's up from 10 percent a year ago.

The problem is that malware, as this and other malicious software is called, gets upgraded faster than antivirus software. "The bad guys can repack and rerelease their malicious code faster than the good guys can build and distribute antivirus signatures to identify and block it," says Joseph E. St. Sauver, manager of security programs for Internet2, an academic-computing consortium.

It's clear that tech security is as much a people problem as it is a technological one. And education and awareness of good computer hygiene are more important than ever to keep networks clean and data safe. The University of Virginia has already received requests from security officials at other colleges who want to borrow the costume.

For more information about maintaining computer wellness at the University of Western Ontario, please visit the **Computer Wellness** site at <http://www.uwo.ca/its/computerWellness.html>



Story with a Happy Ending

Merran Neville <mneville@uwo.ca>

On January 14, Capri, Brian Borowski’s seeing-eye dog, lost one of her blue booties on campus. Brian sent a request to ITS staff to keep an eye out for the booty.

“If people are outside going out the front [of SSB] to the south along Western Road; can you keep an eye out for a blue booty (very small of course for her paws)?”

It so happened that Brian’s colleague John Hickmott was near the Lost and Found items in the Campus Community Police Service Office the next day and checked. There it was and he returned it safely to Brian and Capri, within 24 hours of it being lost. Some anonymous and helpful person had found it and taken it to Lost and Found. Whoever, you are, thank you!



University Hill

Virtual ITRC -->



Instructional Support Team News: Getting Started in Second Life

Kim Hoffman <khoffman@uwo.ca>

Second Life is a 3D immersive virtual world where you can, as your avatar, own land, own buildings, socialize using voice and chat, dance, ski, swim, etc.. You could build your own house, your own car – there's no limit to your creativity! It is much easier to be a millionaire in Second Life – \$1 is roughly equivalent to \$250 Linden.

A number of universities have been teaching in Second Life as a supplement to real life instruction in a traditional classroom setting. Harvard University has had "CyberOne: Law in the Court of Public Opinion" since 2006. The link below will give you an idea of the prerequisites and grading for this course that has a Second Life component.

- Harvard CyberOne Law
<http://www.eecs.harvard.edu/~nesson/e4/>

Others have created educational games.

- Ant DetectiveGame
<http://ca.youtube.com/watch?v=NjKP3Eu3nDY>

With the basic tools available in Second Life, you can create simple objects to illustrate processes, for example,

- Nursing Education
<http://ca.youtube.com/watch?v=l4J7-OlzLV0>

Where to begin

- To learn more about Second Life, go to <http://secondlife.com/>
- To enter the virtual world of Second Life, you will need to create an avatar and download a client onto your computer. The system requirements can be found at <http://secondlife.com/support/sysreqs.php>
- To create an avatar and download the Second Life client click on "GET STARTED" at the top right of <http://secondlife.com/>

ITS has bought an island in Second Life. The university community is welcome to set up projects on this island. To get to the **ITRC at Western** in Second Life, you can teleport to it via an SLURL (this is all one string)

<http://slurl.com/secondlife/ITRC%20at%20Western/215/213/27/?img=http%3A//www.uwo.ca/its/itrc/secondlife/images/sl-western-ITRC.slurl.jpg&title=ITRC%20at%20Western&msg=Welcome%20>

[to%20the%20Instructional%20Technology%20Resource%20Centre%20at%20the%20University%20of%20Western%20Ontario](http://www.uwo.ca/its/itrc/)

Students can access Second Life from the computers in Gen Labs UC2 and NCB 105.

The "Real" ITRC

The real ITRC (<http://www.uwo.ca/its/itrc/>) is located in the Support Services Building, Room 4320 and is open Monday-Friday 10:00am-4:00pm. The ITRC operates within the Client Support area of ITS and works cooperatively with the Teaching Support Center (TSC), Continuing Studies, Distance Studies and Western Libraries to address the need for support for instructional technology. If you are interested in pursuing a project in Second Life please contact its-sl@uwo.ca.

For those who are interested in participating in an event in Second Life, please have a look at events hosted by the International Society for Technology in Education (ISTE) <http://secondlife.iste.wikispaces.net/events>



Professor Mark McDayter's Printer's Devil Project -- Culture of printing and publication in the last half of the seventeenth century in England



Professor Carole Farber's FIMS and Collaboratorium

Upgrading the Outlook Connector

Ryan Renard <rreynard@uwo.ca>

Due to the different timing of development schedules between Microsoft and Sun Microsystems, frequent upgrades to the Microsoft Outlook Connector are needed. As Microsoft releases updates, Sun is often required to release a new version of the Connector in order to update the related code involved with the synchronization features. The reasons for ensuring that you are running the latest version of the Outlook Connector are similar to those of any other product, product enhancement, or patch.

If you are accessing shared calendar content and not running the latest version of the Connector, this could lead to calendar access problems.

Identifying Version and Installation

To identify which version of the Connector you are running, please read the document *How do I ... Check the Version # of the Outlook Connector* at <http://www.uwo.ca/its/doc/hdi/calendar/outlook-version.html>

Instructions for installing the latest version of the Outlook Connector are given online at <http://www.uwo.ca/its/doc/hdi/calendar/outlook.html>

We recommend that a copy of the installation file not be copied to local media for future installations because of the possibility that it may be out-of-date. We appreciate your assistance in this matter.

Data Centre Move Project Team



Left to right: Standing - Jeff Grieve, Eric Cartman, Jon Hickmott, Glen Marrier, Gary Miller, Aaron McDonnell, WeiMei Shyr, Doug Vandevrie, Ken Jorgensen, Ed Zuidema, Martin Douglas, Mark Davis, Chuck Reid, Ed Gibson, Andrew Culver; kneeling - Nancy Wellard, Harold Robson, David Oder, Brian Borowski (with his dog Capri), Steve Reynolds and Brad Wells.



Denis Regnier (above), Jeff Grieve (right)



**NSC237
Lights
Out!**

**Friday, 12
December
2008**

*Debbie Jones,
ITS Director*



*Diane Tillotson, Gerry Semple, Becky Williamson,
Effie Alexis, Barry Kay, Betty Mathers (above); Gary
Miller (right)*



Mike Hulko, Ted Gauci, Merran Neville

Commonly Used Numbers

ITS Support Centre	SSB4100	519 661-3800 ext.83800	<i>helpdesk@uwo.ca</i>
Voice & Data	SSB4100	519 661-3800 ext.83800	<i>helpdesk@uwo.ca</i>
General Office	SSB4300	519 661-2151 ext.82151	FAX No.519 661-3486 ext.83486
Computer Accounts Office	SSB4100	519 661-3800 ext.83800	<i>accting@uwo.ca</i>
Computer & Network Operators		519 661-3525 ext.83525	<i>operator@uwo.ca</i>
IITRC	SSB4320	519 661-2111 ext.85513	<i>itrc-admin@uwo.ca</i>
ITS Non-Credit Courses		519 661-2151 ext.82151	<i>its-courses@uwo.ca</i>
Dial-in Line (all modem speeds)		519 640-5305	
E-mail Postmaster		519 661-3800 ext.83800	<i>postmaster@uwo.ca</i>

Facilities

ITS Support Centre	SSB4100	General Purpose Labs	UC2, NSC110, SH1310
PC Lab	SSB4230		NCB105, SVB13, SVB14,
IITRC	SSB4320		SVB16



Mailing List

If you wish to have your name and/or address added, changed, or deleted from the *In Touch* mailing list, please provide the following information.

Category:

UWO ___ faculty, ___ staff, or ___ graduate student (Please give campus address below.)

Request following action:

___ ADD ___ CHANGE ___ DELETE

Last Name _____ First Name and Initials _____

Department _____

Address of department (Building on campus or affiliate) _____

Previous label information (if varies from above, or include previous label)

Return to: *In Touch* Mailing List, Information Technology Services, Natural Sciences Centre, The University of Western Ontario, London, Ontario, Canada, N6A 5B7