

## *In Touch*

Vol. 12 No. 2

Winter 2005

ISSN 1198-8673

In this issue:

Computer Wellness Campaign	1
Western Quarantine Network	3
ITS Support Centre Team	4
CanIt-PRO: Spam Filtering	5
Shopping Online for the Holidays	6
Instructional Support Team	7

### Computer Wellness Campaign

*Ellen Smout <esmout@uwo.ca>*

The Computer Wellness Committee has launched their second campaign, the **Leave it, Lose it** campaign. This campaign was initiated after a record setting number of laptops were stolen from the D.B. Weldon Library in April 2005. The thefts all occurred when laptops were left unattended in the library by students. These thefts, like most laptop thefts, are preventable thefts.

Laptops and other computer equipment were also stolen from offices, cars, student residences, and computer labs. These thefts cost the University and the individual's time and money and we run the risk of losing sensitive confidential data.

The committee believes that a heightened awareness regarding unattended laptops will result in a lower number of thefts.

In support of this belief, the committee has put posters in various locations at Western including Food Service outlets, Residences, and Western Libraries. The poster can be seen electronically in the Genlabs, the Sun Rays stations and on the WebCT Vista login page and the successful wireless login page.

Visit the Computer Wellness web site for tips on how to safeguard your laptop against theft.

<http://wellness.uwo.ca>

Don't forget about the free Computer Wellness Clinics. E-mail [computer.wellness@uwo.ca](mailto:computer.wellness@uwo.ca) for your appointment.



## Scheduled System Maintenance

Sundays  
6:00am - 12:00 noon

Need help, have a question?

Call the ITS Support Centre  
661-3800 or ext.83800

## 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 ©2005 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,  
Natural Sciences Centre,  
The University of Western Ontario,  
London, Ontario, N6A 5B7

Phone: 519-661-2151  
FAX: 519-661-3486  
Internet: [in.touch@uwo.ca](mailto: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](mailto: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 2005-2006

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

## Western Quarantine Network

Aaron McDonnell <aaronm@uwo.ca>

There once was a time when cleaning a PC with a virus meant grabbing your anti-virus floppy and taking care of it when you had a chance. There wasn't really any sort of threat to worry about since the PC wasn't networked, unless you spotted someone carrying away a floppy from that PC to use in another. Controlling a virus outbreak back then had more to do with one's football tackling abilities to the said disk-carrier than it did to technology.

Today's computer networks present a very different challenge. Western's computer network is a vast system of network hardware, wiring, PCs, servers and fiber lines that link up over 9000 devices. Instead of a thousand known viruses, there are tens of thousands, growing at a rate of hundreds more a month. In fact, viruses are only one of many modern threats a computer faces - now there are rootkits, spyware, malware, worms, trojans, phishing and, of course, the adventurous hacker. Every one of them represents a way in which a PC can be compromised and become a threat to the network that it resides on.

Over the years, Western has placed many monitoring and inspection systems on our network to spot systems that may be compromised by a virus. This allows the ITS NOC group to lock the offending systems until they can be

purged of the malicious code and are no longer a threat to the health of the network. Until now, however, we've never had a good system in place to do the cleaning - the infected PC would have to be fixed offline, then eventually unlocked by the NOC or NSO group when ready.

Enter the new **Western Quarantine Network**. Earlier this year, the NOC group launched a project to create private network space to exist alongside the regular public address space for the various departments. The intent is to provide a network zone that a machine can be moved into, via our RAMP application, which will isolate it from the main

server hands out a new IP number, gateway, and DNS that make use of a sark-box to control things. In addition, access lists placed in the core switches further restrict what can and cannot happen on the Quarantine network, making sure that the infected PCs can only use the systems we intend them to.

The Quarantine network enables a compromised PC to still have connectivity to the Network and Internet for Windows Updates and antivirus updates while simultaneously protecting the rest of the normal network from the influence of compromised systems. Local administrators also gain the ability to unlock the PC themselves once it has been cleaned. The ease of patching

and updating a system, and unlocking it locally on

**The Quarantine network enables a compromised PC to still have connectivity to the Network and Internet for Windows Updates and antivirus updates while simultaneously protecting the rest of the normal network from the influence of compromised systems.**

this new network minimizes downtime while protecting the rest of the network from attack of malicious software.

Quarantine

Networks have been rolled out now to about half of the networks that require them, with the other half soon to come. We hope that it will make it easier for everyone in dealing with a compromised PC, and help to keep Western's network a reliable and good experience for all that use it.

network where it can be controlled, but still allow some connectivity so that the machine can be cleaned quickly and easily without being a danger to other systems.

To automate this process, something was needed to control the access that these machines would have, so a series of servers bearing the name "sark" were created to act as the gateways and DNS servers for this special Quarantine network. When a machine is moved to this network, via the RAMP application, the DHCP



*Candy Shum, Rob Dykeman, Rob Davis, Matt Bramham, Matt Simmons, Rob Atkinson,*

## ITS Support Centre Team

*Judy Steward <judy@uwo.ca>*

The ITS Support Centre consists of the Help Desk and the Computer Accounts Office. We provide support for Western's faculty, staff and students, which includes

- first level technical support for PCs and MACs
- first level technical support for voice and data problems
- troubleshooting for dialin and on-campus connections including e-mail, internet access, etc.
- software support for ITS Supported Software
- dispatch of second level technicians for on-campus support
- general questions about computing at Western and available support resources

The Support Centre offices are located on the 2nd floor of Natural Sciences and are open for drop in support from 8:30 a.m. to 4:30 p.m. from Monday to Friday. The phone number is 661-3800, ext.83800. Questions can also be e-mailed to us at [\*\*helpdesk@uwo.ca\*\*](mailto:helpdesk@uwo.ca).

### Full time Support Centre Staff (with primary areas of support)

- Effie Alexis - Computer Accounts Office
- Rob Atkinson - Wireless Clinics, Wireless web site
- Matthew Bramham - JES

### Deployment Coordinator

- Rob Davis - Wellness Clinics, Wellness web site (with Ellen Smout)
- Rob Dykeman - Genlabs
- Andrew Filippi - Computer Accounts Projects
- Vince Lombardi - Help Desk E-mail, WebCT Vista
- Candy Shum - Applications Development
- Matt Simmons - Postmaster, Webmaster
- Judy Steward - Team Leader, Site Licenses, TUMS, Global Dialer
- Richard Towle - Computer Accounts Office

Photo: Chan Yin



Richard Towle, Vince Lombardi, Andrew Filippi, Effie Alexis, Judy Steward (Team Leader)

## CanIt-PRO: Spam Filtering System

Eric Cartman <eric@uwo.ca>

### Part time Support Centre Staff

Bill Anstice  
Will Beldman  
Jateen Bulsara  
Babtunde Cole  
Andrea Domokos  
Hicham El-Chazli  
Amy Ferguson  
Andrew Nemirovsky  
Karin Palmer  
Melissa Weston

You have probably noticed a reduction in SPAM passing through the Western e-mail system since the fall. In September, ITS began testing a new SPAM filtering system called CanIt-PRO from Roaring Penguin Software Inc. During this testing phase, all e-mail addressed to @uwo.ca recipients passed through this new filter. A group of ITS staff volunteered for full filtering, while e-mail for the rest of our accounts passed through to the existing production system. While these e-mails were not SPAM checked, a cross check of the sender was performed, requiring new senders (those not previously encountered by the system) to resend, thus verifying that the sending host was, in fact, a real

mail server and not a “SPAM cannon”.

The new system, still in testing, will be phased into full production early in 2006, bringing a slate of new features to handle SPAM. UWO mail users will be able to have suspect mail quarantined. Notification of quarantine contents will be e-mailed daily to the user.

The freedom of self management will allow for user-customized rules. Customization will be made available to the user through a secure web interface, accessed with the same username and password used for Western authentications now.

You can expect to receive news about the phasing in of this exciting new service in your e-mail as we enter each stage on our way to full production.

## Shopping Online for the Holidays: Twelve Tips to Protect Yourself From Cyber Grinches, Scams and Schemes

*Editor's Note: This article is reprinted from STAYSAFEONLINE.org at [http://www.staysafeonline.info/news/press\\_nov17\\_2005.html](http://www.staysafeonline.info/news/press_nov17_2005.html)*

Press Contact:  
Julie Han  
415-975-3327  
[jhan@porternovelli.com](mailto:jhan@porternovelli.com)

The National Consumers League, the National Cyber Security Alliance and the Better Business Bureau Provide Joint Advice on Safe Online Shopping Do's and Don'ts

### WASHINGTON, DC November 17, 2005

The holiday season is a busy time as people hunt for the perfect gifts for family and friends. The Internet can make your shopping faster and easier, but there can also be pitfalls if you're not careful. The National Consumers League, the Better Business Bureau and the National Cyber Security Alliance offer key advice to ensure you have a safe online shopping experience, so that your gift-giving is a joyous occasion, not an opportunity for cyber thieves:

1. Know who you're dealing with. Check out unfamiliar sellers with the Better Business Bureau and your state or local consumer protection agency. If you're buying gifts on an online auction site that provides a feedback forum, check the track record of the seller before you bid. Don't buy things in response to unsolicited emails from unknown companies, since these may be fraudulent.

2. Get all the details. Get the name and physical address of the seller; how much the product or service costs; what

is included for that price; whether there are shipping charges; the delivery time, if any; the seller's privacy policy; and the cancellation and return policy.

3. Look for signs that online purchases are secure. At the point that you are providing your payment information, the beginning of the Web site address should change from **http** to **shhttp** or **https**, indicating that the information is being encrypted — turned into code that can only be read by the seller. Your browser may also signal that the information is secure with a symbol, such as a broken key that becomes whole or a padlock that closes.

4. Pay the safest way. It's best to use a credit card, especially when you're purchasing something that will be delivered later, because under federal law you can dispute the charges if you don't get what you were promised. You also have dispute rights if there are unauthorized charges on your credit card, and many card issues have "zero liability" policies under which you pay nothing if someone steals your credit card number and uses it.

5. Never enter your personal information in a pop-up screen. When you visit a company's Web site, an unauthorized pop-up screen created by an identity thief could appear, with blanks for you to provide your personal information. Legitimate companies don't ask for personal information via pop-up screens. Install pop-up blocking software to avoid this type of scam.

6. Keep documentation of your order. When you've completed the online order process, there may be a final confirmation page and/or you might receive confirmation by email. Print that information and keep it handy in case you need it later.

7. Know your rights. Federal law requires orders made by mail, phone or online to be shipped by the date promised or, if no delivery time was stated, within 30 days. If the goods aren't shipped on time, you can cancel and demand a refund. There is no general three-day cancellation right, but you do have the right to reject merchandise if it's defective or was misrepresented. Otherwise, it's the company's policies that determine if you can cancel the purchase and whether you can get a refund or credit.

8. Be suspicious if someone contacts you unexpectedly and asks for your personal information. Identity thieves send out bogus emails about problems with consumers' accounts to lure them into providing their personal information. Legitimate companies don't operate that way.

9. Check your credit card and bank statements carefully. Notify the bank immediately if there are unauthorized charges or debits, if you were charged more than you should have been, or if there are any other problems.

10. Keep your computer secure for safe shopping and other online activities. Protect your computer with spam filters, anti-virus and anti-spyware software, and a firewall, and keep them up to date. Go to [www.staysafeonline.org](http://www.staysafeonline.org) and [www.onguardonline.gov](http://www.onguardonline.gov) to learn more about how to keep your computer secure.

11. Beware of emails offering loans or credit, even if you have credit problems. Con artists take advantage of cash-strapped consumers during the holidays to offer personal loans or credit cards for a fee upfront. These scammers simply take the money and run.

12. Contact the seller promptly about any problems with your order. Check the company's Web site for a customer service page, "contact us" link, email address, or phone number to get your complaint addressed or questions answered. If you can't resolve the problem, contact the Better Business Bureau or your state or local consumer protection agency for help.

These tips are available at [www.nclnet.org/holiday](http://www.nclnet.org/holiday) or [www.staysafeonline.org](http://www.staysafeonline.org). NCL offers advice about shopping safely online at [www.nclnet.org/shoppingonline](http://www.nclnet.org/shoppingonline) and telemarketing and Internet fraud tips at [www.fraud.org](http://www.fraud.org). The BBB offers reports on several million businesses at [www.bbb.org](http://www.bbb.org) and access to nearly 25,000 BBBOOnline seal holders, plus consumer and business tips at [www.bbbonline.org](http://www.bbbonline.org).

## Other articles on this topic

### *Majority of U.S. Adults Believe They Are More Susceptible to Identity Theft During the Holiday Season*

<http://biz.yahoo.com/prnews/051122/sftu041.html?v=35>

### *Online shoppers say criminals won't take holiday*

[http://today.reuters.com/business/newsarticle.aspx?type=reutersEdge&storyID=2005-11-23T175626Z\\_01\\_FLE358468\\_RTRUKOC\\_0\\_US-ECONOMY-CONSUMERS-IDTHEFT.xml](http://today.reuters.com/business/newsarticle.aspx?type=reutersEdge&storyID=2005-11-23T175626Z_01_FLE358468_RTRUKOC_0_US-ECONOMY-CONSUMERS-IDTHEFT.xml)

## ITS Instructional Support Team

Merran Neville <[mneville@uwo.ca](mailto:mneville@uwo.ca)>

The instructional support team is made up of four ITS staff members and the eleven student developers in the ITRC. The ITS staff are Sue Barschel, Jeff Longland, Merran Neville, and Jane Winkler. The ITRC student developers are Michelle Bauer, Sam Chow, Andrew deWaard, Zlat Djuric, Nick Greven, Nick Haffie-Emslie, Bryce Hunter, Rahim Kanani, Chan Yin, Angela Vandenbogaard, and Jon Villalobos.

The team assists faculty with instructional projects using technology, creating Vista courses, and training in the use of Vista. Technology support is provided to the Teaching Support Centre located in the D.B. Weldon Library, room 122. Drop-in assistance and telephone support is given in the ITRC located in Natural Sciences room 118 and the Teaching Support Centre.

The four ITS staff members are project leaders responsible for managing the ITRC projects for their assigned faculties and are contacts for Vista support in these faculties.

## Contact List for Faculty Support

### Sue Barschel

Information & Media Studies  
Social Science  
Collaborative Interdisciplinary Programs  
Brescia University College  
Administration (HE)

### Jeff Longland

Arts & Humanities  
Law  
Science  
Distance Studies  
Western Centre for Continuing Studies  
Western Libraries  
Administration (HR)

### Merran Neville

Education  
Engineering  
Graduate Studies  
Music  
Huron University College

### Jane Winkler

Health Sciences  
Medicine & Dentistry  
Richard Ivey School of Business  
Western Libraries  
King's University College  
Outreach Program

Several new projects were received during the Fall project submission period. Although projects are generally submitted in October and March, they will continue to be accepted throughout the year. The new projects are being assigned to the ITRC student developers and many present new and exciting challenges to the group.

The four ITS staff members, together with Client Support Manager Jean Savage, have begun a series of presentations to faculties and departments which highlight the activities of the ITRC and the support available to faculty. Three such presentations have been given so far and more will be scheduled in the new year.

Questions about Vista can be e-mailed to [ITS-Vista-wg@uwo.ca](mailto:ITS-Vista-wg@uwo.ca); all other questions can be e-mailed to [itrc-admin@uwo.ca](mailto:itrc-admin@uwo.ca).