University of Oregon

COMPUTING NEWS

Winter 2006

The Cape Blanco Lighthouse shrouded in winter fog. Cape Blanco is the westernmost point in Oregon.The lighthouse was constructed in 1870. Its lamp at the top of the 59-foot tower reaches 245 feet above sea level.

IN THIS ISSUE…

Email

Networking

Microcomputing

Web

Security

Statistics

People

Interesting Sites

Educational Technology

IT Training

New Options for “Vacation Mail” Auto-responder

New web-based interface and TINYVAC program for PROCMAIL give UO users new options for creating automatic “on vacation” email responders

If you’ve been looking for an easy way to create an automatic email response message when you’re on vacation, you now have a couple of new options for your uoregon.edu account.

The easiest method of setting up an automated responder is by filling out the interactive form at **https://password.uoregon.edu/vacation/**

You may also access this form by clicking the “auto-responder” link at the bottom of the UO Web Email page at **http://email.uoregon.edu/**

For those who prefer to use PROCMAIL and the PICO text editor, we’ve scripted a new program called TINYVAC to assist you in creating and managing automated vacation messages.

The TINYVAC script installs a copy of the system default rc.vacation file in your home directory ($ HOME) To activate the program for the first time, log in to your uoregon.edu account via ssh and type

```
% tinyvac
```

You’ll be presented with a list of options and some usage notes. Enter Options 1, 2, and 3 in succession at the prompts, e.g.:

`Enter Option >>> 1` *(this sets up PROCMAIL to use rc.vacation)*`...`

`Enter Option >>> 2` *(this turns rc.vacation ON)*`...`

`Enter Option >>> 3` *(this lets you edit your vacation message)*

For more details on how to use TINYVAC, including links to complete documentation, sample messages, and editing tips, see **http://www.uoregon.edu/~llynch/tinyvac/**

UNIVERSITY OF OREGON

COMPUTING CENTER

COMPUTING NEWS

VOL. 21 #1

Computing News is published quarterly by the User Services and Network Applications staff of the Computing Center.

© University of Oregon 2006

Contact: Joyce Winslow
jwins@uoregon.edu

Photography: Dave Ragsdale
dave@uoregon.edu

Joe St Sauver, Ph.D.
Director, User Services
and Network Applications
joe@uoregon.edu

Website:
http://cc.uoregon.edu/cnews/

Telephone: (541) 346-1724

Got Extras?

If your campus department receives surplus copies of *Computing News*, you may return them to the UO Computing Center for redistribution.

Opportunities to Apply for Educational Technology Funds

Deadline for classroom equipment requests is February 15, 2006

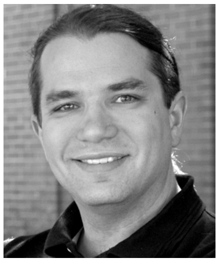
During the 2005/06 academic year, there will be several opportunities for campus units and faculty members to apply for educational technology funds. The funds will be used to make targeted investments in classroom technology, large-scale infrastructure initiatives, and curriculum development.

Classroom Equipment Proposals. Currently, the Educational Technology Committee has issued a call for classroom equipment proposals, and worksheets for describing individual departmental needs have been distributed to UO deans, department heads, and program directors. The UO Libraries Media Services Department has developed standard packages of classroom equipment suitable for different spaces, and you are encouraged to discuss your department’s needs with Media Services staff before filling out a worksheet. If your department requires additional equipment, you may describe those needs in the worksheet.

Email or deliver completed worksheets to Terri Warpinski, Vice Provost for Academic Affairs and Chair of the Classroom Committee (*tlw@uoregon.edu;* 206 Johnson Hall). Once these requests have been evaluated and prioritized, purchasing and installation may begin spring term 2006.

Watch for Calls for Other Proposals. Calls for other Ed Tech fund proposals will be made early winter term. Visit the Ed Tech website at **http://libweb.uoregon.edu/edtech/** for future announcements.

Get Acquainted with Network Security Services



The Computing Center's Network Services now offers security assistance to campus departments

Josh Ward
Security Engineer
jward@uoregon.edu

Recognizing that many departments on campus lack the necessary staff to properly maintain a departmental firewall or other security appliances, Network Services recently began offering managed security services to the campus community. Now you can get professional assistance to help keep your departmental computers and data secure and safe.

Risk Assessment

The first step in a managed firewall deployment is identifying the assets that need protection. Network Services can help each department quantify the following things:

- What type of data is your organization storing and serving?
- Who is the data being served to?
- Where is the data being stored?
- How sensitive is this information itself?
- What are the political and financial consequences should a breach occur?

Protection Selection

Once assets requiring protection are quantified, Network Services will assist you in selecting the best hardware and software to keep you safe. Depending on your needs and budget, we can specify and purchase firewall hardware, virtual private network (VPN) hardware, Intrusion Prevention System (IPS) products, or any other security device that is indicated. Depending on your needs, Network Services can build a secure network with the same redundancy as the campus network.

By using our managed security services, you also leverage our relationships with security vendors. We manage everything—including purchasing, deploying, maintaining software, and maintaining hardware.

Security Policy

After all of the necessary equipment to protect your department is procured, we work closely with local administrators to formulate the best security policy for you. This includes protocol analysis for each of your servers to determine what access is needed for the "least-access" principal to apply. This involves deploying the most restrictive policies that will allow you to continue operating.

After the policy is selected, we prototype and tune the rules in-place on the firewall or IPS without interrupting normal network operation. This ensures a smooth transition into a more secure network infrastructure. During this final deployment phase, local administrators are also involved to ensure that no critical services were overlooked during the initial inventory of servers.

Security Awareness

Network security is only as strong as its weakest link. If someone breaks into a server exposed through the firewall, that server may be used to "leap-frog" into other servers or workstations with sensitive information. Network Services can work with your employees to help increase overall knowledge about electronic security. By working with local administrators we can help to make them aware of attack vectors. This will ensure that they are aware of any exposure to the Internet and understand what measures should be employed to mitigate threats.

Ongoing Services

Network Services staff continue to involve themselves in the security operations of your group. We conduct ongoing meetings with local department administrators to ensure that the firewall, VPN, and IPS policies continue to meet your operational needs. We make sure that the software on your deployed security devices is up-to-date and properly configured.

In addition to the ongoing policy and maintenance services we offer, we can provide local administrators with vulnerability reports. We have dedicated hardware that will probe servers protected by our security devices to determine if, despite the installed protection, servers may still be vulnerable to a specific exploit. We will work with the local administrators to mitigate any vulnerabilities discovered by our scanning.

Most users on campus know that the Internet is no longer a safe place. We must be vigilant and protect ourselves at all times, but many users lack the knowledge to protect themselves. By using our services to help make your network more secure, you can provide additional layers of protection for your user population.

If you'd like to further discuss our service offerings, please email *security@uoregon.edu*. Include a brief description of your needs and we'll see what we can do to help.

Pricing for our security services varies depending on the complexity of the deployment. For specific pricing information, contact Network Services Director Dale Smith (*dsmith@uoregon.edu*).

Instructional Technology Fellows

IT award enables six UO faculty members to further their development of advanced technology teaching tools

Ron Renchler
Director, Library Communications
UO Libraries
ronr@uoregon.edu

With funding from the Instructional Technology Resident Fellowship Program sponsored by the UO's Office of Academic Affairs, six university faculty members are now in the process of creating cutting-edge instructional technology (IT) tools while simultaneously mentoring students and faculty members in IT development.

Fellows will spend several weeks working closely with a supporting IT unit on campus to develop an array of classroom and online teaching and learning tools. All tools will be designed to have applications to larger segments of the campus community. IT fellows will spend a term in residence with their sponsoring unit developing project components and advising and mentoring other faculty members.

2005-6 IT Fellows and Their Projects

Nancy Cheng, Architecture

Topic: "Visual Thinking with Digital Sketches"

Sponsoring IT Unit: Wired Humanities Project, Judith Musick, Director

To help design students describe, interpret, and shape visual ideas, Nancy Cheng has been collecting animated sketches using the Anoto digital pen-and-paper system. The animated drawings offer a stroke-by-stroke view of how designers think. By interactively viewing the animations, students can study how experts approach tasks such as space planning or façade design.

Cheng will work with the Wired Humanities Project group to make the drawings accessible through a web database and develop prototypical classroom lessons.

Suzanne Clark, English

Topic: "The New Research: A Guide"

Sponsoring IT Unit: Metadata and Digital Library Services,

Carol Hixson, Head

Suzanne Clark's project will help UO students connect the rhetorical processes of inquiry, interpretation, and argument to the rich research guides and technologies librarians have developed over the last few years. It will be tested for use in sections of Writing 123, The Research Paper, and in other writing programs at the university.

Staff members in the UO Libraries' Metadata and Digital Library Services will consult with Clark on the research uses of several recently developed online tools, including Scholars' Bank, an institutional repository for the intellectual output of the university.

Kevin Hatfield, Central Oregon Programs

Topic: "Teaching History at a Distance through IP Video Broadcasts"

Sponsoring IT Unit: Media Services, Tom Matney, Director

Kevin Hatfield is developing a curriculum for students earning a history minor at the Bend campus. His project will include the redesign of history courses for a broadcast format and development of archived material for video-on-demand delivery, with the goal of developing broadcast courses that retain the interpersonal advantages of on-site delivery while incorporating hybrid elements that enhance student learning. He will also share his expertise in broadcast pedagogy with other UO faculty members through mentoring and collaboration. Media Services, housed at the UO Libraries, will provide assistance in meeting broadcast-quality delivery standards.

Named for 2005-6

Mark Horney, Educational Studies

Topic: "Supporting the College of Education Faculty"

Sponsoring IT Unit: Center for Educational Technologies, JQ Johnson, Director

Mark Horney teaches IT courses in the Teacher Education Area and provides IT training for many adjunct and regular College of Education faculty. His project will concentrate on using IT resources to train and support education instructors, especially in the advanced use of Blackboard, the university's course management system. An immediate focus will be on developing learning objects to train instructors to create and post their own video material on Blackboard. A second area of concentration will be the creation of several online courses, along with the development of computer-mediated techniques for mentoring and discussion group activities. The Center for Educational Technologies will provide staff consultation and software and hardware support.

Kartz Ucci, Art
Topic: "Teaching Visual Literacy: Improved Skills for Students and Faculty"
Sponsoring IT Units: Center for Educational Technologies, JQ Johnson, Director; Teaching Effectiveness Program, Georgeanne Cooper, Director

Kartz Ucci will use her fellowship to integrate digital art content into a series of courses, workshops, and online teaching models that will increase learning opportunities and elevate visual literacy skills among students and faculty members. Ucci will create online components for digital art courses and seamlessly integrate them into Blackboard's interface. Overall, she plans to develop a course model that combines classroom teaching and online elements that can be used in large format introductory and foundation courses at the UO. Ucci will collaborate with the Center for Educational Technologies and the Teaching Effectiveness Program to develop workshops on creating and using media-rich tools for learning and instruction.

Catherine Wiebe, Romance Languages

Topic: "Building Better Tools for Language Instruction"

Sponsoring IT Unit: Yamada Language Center, Jeff Magoto, Director

Catherine Wiebe oversees curriculum development for French courses taught to more than 250 UO students each term. She will use her fellowship to redesign elements of the second-year French program to include dynamic online instructional components for form (listening, reading, speaking) and content (grammar, vocabulary). The resulting hybrid-style course will allow students to supplement three hours of classroom instruction each week with one hour of interactive, online instruction. Wiebe will develop instructional templates and build video and audio databases for online delivery of the language instruction material. Yamada Language Center staff will supply technological expertise, logistical support, and hardware and software consultation.

More Information About IT Fellowships at the UO

A companion series of summer workshops for faculty interested in learning more about using IT in their classes will be held in summer 2006. Descriptions of the faculty IT development workshops and application materials is available at **http://oaa.uoregon.edu/itif/** Review of workshop applications will begin January 15, 2006, and continue until openings are filled.

Information about the 2006-7 Instructional Technology Resident Fellowships is available at **http://oaa.uoregon.edu/itif/** Review of applications will begin February 1, 2006.

Who's Who at the Computing Center

Meet our video conferencing administrator…

Joyce Winslow
jwins@uoregon.edu

Craig Leavy, Telecommunications Services Video Conferencing Administrator

Ask Craig Leavy about his job as a video conferencing engineer at Telecom Services and his eyes sparkle with enthusiasm. Craig is especially enthused about the role video conferencing technology plays in distance learning. "I'm a firm believer in the power of education to change people's lives," he says emphatically, "and visual learning is very important—it's so effective!"

Aside from the technology's ability to bring students and teachers together across great distances, Craig also likes the fact that video conferencing is economical. It saves both money and time, allowing administrators, teachers, and others to meet with each other without the expense and disruption of travel. Video conferencing is also widely used as a tool for screening job candidates—yet another cost-saver.

Since Craig began his job at the UO ten years ago, he's seen video conferencing technology evolve from a complex setup to a simple "plug-and-play" system. The technology is now so user-friendly that almost anyone can set up a video conference from a networked computer without much assistance.

To be effective, however, a video conference needs more than the appropriate hardware, software, and engineering technique. Lighting, sound, and attention to visual detail all contribute to the success of a project. This is where Craig's deep background in video production is a real plus. Before joining Telecom Services in the fall of 1995, Craig worked for 12 years as a full-time video producer at Lane Community College, where he earned dual degrees in radio and TV broadcasting and broadcast electronics after graduating from OSU with a B.S. in political science. His interest in documentary filmmaking, which dates back to his undergraduate days at OSU, and his passion for cinema in general have undoubtedly also contributed to his discerning eye.

Craig is so enthusiastic about his job, you might think he has time for little else, but in fact he is equally enthusiastic about a lot of things. Music, for instance. Craig calls music his "number one hobby," and he has a huge collection of recorded music, including old 78s, vinyl LPs, and even 8-track, cassette, and reel-to-reel tapes, "plus an ever growing number of CDs." Craig, who modestly describes himself as "a bad guitar player," is an avid concert-goer and cites Peter White and Craig Chaquico among his long list of current inspirations.

Growing up in the lush green countryside outside Corvallis, this Willamette Valley native also developed an enduring affection for water sports—and dogs. Whenever possible, he has made his home near a body of water, and he has rarely been without canine companionship in his life. Craig currently enjoys the best of both worlds: living on the shores of Fern Ridge Lake with his Springer Spaniel Mocha, who is always eager to accompany him on his frequent fishing and boating adventures.

nsrc in the news

The UO-based Network Startup Research Center (NSRC) was cited in an article recently published by the San Diego Supercomputing Center (SDSC) regarding a network monitoring project of the National Laboratory for Applied Network Research (NLANR). The article describes the collaborative efforts of NLANR researchers and the NSRC to monitor and analyze vital international networks to help improve their performance by assisting in the deployment of the first Active Measurement Project (AMP) monitors in Africa. For full details, see "SDSC Networking Active Measurement Project Expands to Africa" at

http://www.sdsc.edu/Press/2005/11/110205_amp.html

New Web-based UO Alpha Mail Offers Many User-Friendly Features

Foreign language compatibility, quick and easy spam reporting, and convenient searching and customizing options are just a few reasons to like Alpha Mail

Many of the early testers of Alpha Mail, the UO's new secure web-based email option, have liked it so much that they are now using it exclusively for all their email needs.

Alpha Mail is still in the process of being enhanced in response to user feedback, but it is already full-featured and ready to use. If you want to try it, go to **http://email.uoregon.edu/** and select the link ***New!*** *New web email (alternative interface to your uoregon.edu account)*. You'll be presented with a login page that asks for your uoregon.edu username and password.

After you've successfully logged in to Alpha Mail for the first time, you'll see a request to set your initial preferences (your addressing preference, how you wish to handle sent mail and deleted mail, and the mail folders you wish to have displayed). You can change any of these choices later by simply opening the Settings menu at the top of the page and selecting new preferences.

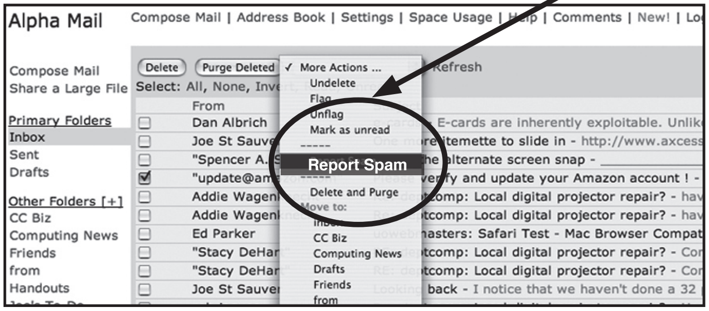
After you've established your initial preferences, subsequent Alpha Mail logins will take you directly to a list of messages in your Inbox. By using the Settings menu, you may choose the number of messages to display per page. Unread messages appear in green. Once you've replied to a message, a green letter R will appear to the left of it. If you flag a message, it's displayed in red for quick reference. (To flag a message, select it by clicking the checkbox, open the More Actions menu—which is directly above/below the mailbox index—and choose Flag.)

At the top of the Alpha Mail page is a row of frequently used menu items, such as Compose, Logout, Settings, and Address Book. In the left margin of the page, you'll see the list of mail folders you've chosen to display. These features are fairly standard and are probably already familiar to you from other mail programs you've used.

Special Features

In addition to the more familiar features described above, you'll find some welcome additions that can make your email correspondence and message management extremely convenient:

1. **Sharing Large Files.** Alpha Mail can send files up to 200MB. To set the parameters for this service and send the file, open the Share a Large File link in the left menu and fill in the blanks.
2. **Foreign Language Capability.** Alpha Mail is 100% Unicode compliant and can handle all your foreign correspondence needs, whether you're sending email in Polish, Pushto, Thai, or Gujarati. You can also create folder names in any language you wish.
3. **Quick View of Disk Quota Usage.** No need to get caught short on disk space! You can easily monitor your disk space usage by clicking the Space Usage link at the top of your Alpha Mail page. Disk use information is updated every five minutes.
4. **Easy Spam Reporting.** You can quickly and easily report spam in two steps:
   - Open the mailbox index list and check the box(es) next to the offending message(s)
   - Click the More actions... button at the top/bottom of the message list, select Report Spam, and hit Return.


Alpha Mail
Compose Mail | Address Book | Settings | Space Usage | Help | Comments | New! | Lo
Compose Mail
Share a Large File
Primary Folders
Inbox
Sent
Drafts
Other Folders [+]
CC Biz
Computing News
Friends
from
Handouts
Delete
Purge Deleted
✓ More Actions ...
Undelete
Flag
Unflag
Mark as unread

Report Spam

Delete and Purge
Move to:
Inbox
CC Biz
Computing News
Drafts
Friends
from
Refresh
Select: All, None, Inve
From
Dan Albrich
Joe St Sauve
"Spencer A. S
"update@am
Addie Wagen
Addie Wagen
Ed Parker
"Stacy DeHar
"Stacy DeHar
Joe St Sauver
E-cards are inherently exploitable. Unlik
itemette to slide in - http://www.axcess
he alternate screen snap -
verify and update your Amazon account ! -
tcomp: Local digital projector repair? - hav
tcomp: Local digital projector repair? - hav
asters: Safari Test - Mac Browser Compat
tcomp: Local digital projector repair? - Cor
tcomp: Local digital projector repair? - Cor
back - I notice that we haven't done a 32

   You'll see a confirmation that your spam was reported, highlighted in yellow at the top of the page. That's all there is to it!
5. **Optional Trash Can.** If you prefer to delete and purge your messages directly from the mailbox index page instead of storing deleted messages in the Trash Can, you can set that option under Settings -> Folders. Under Utility Folders->Trash Folder, simply choose "None (delete messages on purge)." Thereafter, the messages you choose to delete will be displayed with a line through them in the mailbox index. To delete them permanently, hit the Purge Deleted button at the top/bottom of the mailbox index page.
6. **Message Filtering.** Type keywords in the Filter box in the upper right corner of your mailbox index to display only those messages that match. Filtering instructions and examples appear when you hover over the Filter box with your mouse.
7. **Address Book Importing.** You can easily import your address book from UO "Green" WebMail and many other email clients by going to Address Book-> Import and following the instructions.

These are only some of the handy features of Alpha Mail, and more refinements are still being added. Give Alpha Mail a try and find out why it's becoming the email client of choice for many UO users.

Be Wary of Electronic Greeting Cards

Know how to spot a phony e-card, and be sure you can authenticate the sender

Dan Albrich
Manager, Microcomputer Services
dalbrich@uoregon.edu

Over the holidays, you may have seen more online greeting cards (e-cards) in your mailbox than usual. Instead of a friendly communiqué from a well-wisher, however, an e-card is often the delivery system for computer viruses and spyware.

The safest practice would be to avoid e-cards entirely, but if you must send and receive e-cards, be sure to follow some basic safety precautions. Manually enter URLs instead of clicking on them, or cut-and-paste them to avoid common misdirection ploys. Always avoid downloading and then double-clicking on anything!

How to Identify a Bogus E-Card

ScamBusters.org (**http://www.scambusters.org/ecards.html**) has some useful suggestions for identifying a bogus e-card. Here are some of the most common tip-offs they mention:

- **Spelling mistakes** (e.g., "Congratulation!", or a misspelling of your name).
- **Errors in the message** (e.g., the message says you sent a card instead of receiving one).
- **The sender isn't someone you know.**
- **The sender has a bogus name** (Joe Cool, Agatha Tragonawar, Card Sender, Secret Admirer, etc.).
- The URL appears odd (e.g., **www.http://** instead of **http://www**).

How to Avoid Trouble from Fake E-Cards

ScamBusters also lists some common-sense rules for avoiding trouble from fake e-cards:

- **When in doubt, don't open an e-card.**
- **Immediately delete any e-card from someone you don't know.**
- **Never click on anything from an unknown source, never open an attachment from an unknown source, and never download from an unknown source.** (It's really as simple as that!)
- **Never click to accept terms from any company without reading the fine print.** The fine print in one e-card scam actually asked users to allow the company to access their address book and forward a message to everyone in it!
- **Use antivirus software and keep it up-to-date.** (The UO has a site license for McAfee Antivirus software; see **http://micro.uoregon.edu/av/mcafee.html** for more information on how to get and install your copy of McAfee.)
- **Avoid Internet Explorer.** Many e-card scams exploit loopholes in Internet Explorer, so it's best to use Mozilla Firefox (**http://www.mozilla.com/**) instead. Be sure to keep Firefox updated to protect against exploits.
- **Don't open any e-card that contains an attachment.** You never know what is really in that attachment until it's too late.
- **Be skeptical and alert.** If something seems fishy, be cautious. Remember, a Trojan virus can make a phony e-card look like it's coming from a friend or family member.

The Safest Bet is to Avoid Using E-Cards Entirely

E-cards are inherently exploitable. Unlike a simple email message, e-cards require the user to click on a URL or an image to be viewed. For this reason, the safest bet is to avoid sending and using e-cards.

Want to Learn More about Web Publishing?

If you're involved in web publishing on campus, you may want to join the Web Mechanics Mentoring Group.

The group meets on the third Wednesday of each month at 12 noon in 235 Knight Library to discuss current topics of interest to web developers. Interested UO staff, faculty, and students are invited to subscribe to the Web Mechanics' listserv and attend any of the group's meetings.

For more information, including topics of discussion, seminar schedules, and a link to the group's listserv, go to **http://webmechanics.uoregon.edu/**

Contact Richard Hadley (*rhadley@uoregon.edu*) if you have further questions.

FAQs: The Many Names of the Server Formerly Known As Darkwing

In the old days, when everything ran on a pair of monolithic servers known as darkwing.uoregon.edu and gladstone.uoregon.edu, you could access almost any service by referring to the name of the system you were on. But now that we've consolidated and upgraded Darkwing and Gladstone to be uoregon.edu, server names generally refer to the service provided. For example, the IMAP server's name is imap.uoregon.edu, and the SMTP server's name is smtp.uoregon.edu While that's pretty straightforward, some have asked for a summary of the correct names to use when accessing uoregon.edu-based services. We're happy to help clear that up with this article.

My uoregon.edu account itself

Q. What do I call my account on the new consolidated darkwing/gladstone?

A. Refer to your "uoregon.edu account"

Email

Q. What's my email address on the new system?

A. If your old email address was
jersmith@darkwing.uoregon.edu or
jersmith@gladstone.uoregon.edu or
jersmith@oregon.uoregon.edu
you should begin referring to your email address as jersmith@uoregon.edu Mail sent to your username at any of the three old hostnames will also continue to be delivered to your uoregon.edu account for the foreseeable future.

Q. Can I drop the .edu from the end of my address? Or what if my email program 'guesses' my email address to be jersmith@imap.uoregon.edu or jersmith@pop.uoregon.edu? Is that okay?

A. No. Just to clarify this by example:

jersmith@uoregon.edu	<— CORRECT and recommended
jersmith@darkwing.uoregon.edu	<— (deprecated)
jersmith@gladstone.uoregon.edu	<— (deprecated)
jersmith@oregon.uoregon.edu	<— (deprecated)
jersmith@uoregon	<— WRONG, don't use
jersmith@pop.uoregon.edu	<— WRONG, don't use
jersmith@imap.uoregon.edu	<— WRONG, don't use

Q. I want to access my uoregon.edu email via the web. What page do I go to?

A. http://email.uoregon.edu/

Q. What's the name of the uoregon.edu IMAP server?

A. imap.uoregon.edu (see **http://micro.uoregon.edu/email/** for additional important configuration information)

Q. What's the name of the uoregon.edu SMTP (outgoing email) server?

A. smtp.uoregon.edu (if you're connecting to your account from a commercial ISP such as Comcast, Qwest, or AOL, set your SMTP server to whatever they recommend, or run UO's VPN software as described at **http://micro.uoregon.edu/getconnected/vpn_overview.html**)

Q. What's the name of the uoregon.edu POP server?

A. pop.uoregon.edu (Note: we strongly recommend using web email or IMAP instead of POP.)

World Wide Web

Q: How about web pages on my uoregon.edu account?

A: If you had a web page that was formerly at
http://darkwing.uoregon.edu/~jersmith/abc.html or
http://gladstone.uoregon.edu/~jersmith/abc.html
you should replace darkwing.uoregon.edu or gladstone.uoregon.edu with www.uoregon.edu and begin referring to that same web page as
http://www.uoregon.edu/~jersmith/abc.html

Old links to Darkwing or Gladstone: Your old URLs will continue to work for the foreseeable future, but you should begin updating any references to your web page to www.uoregon.edu instead.

Q. What about dropping the whole darkwing/gladstone/www thing entirely and using URLs such as http://uoregon.edu/~jersmith/abc.html instead?

A. Please do *not* do that; in the future it may result in your uoregon.edu web pages becoming inaccessible. Here are some examples of correct and incorrect URLs:

http://www.uoregon.edu/~jersmith/abc.html
CORRECT and recommended

http://darkwing.uoregon.edu/~jersmith/abc.html
(deprecated)

http://gladstone.uoregon.edu/~jersmith/abc.html
(deprecated)

http://uoregon.edu/~jersmith/abc.html
WRONG, don't use

Shell Access

Q. I use ssh to do work at the percent sign or dollar sign shell prompt. What name should I use for that?

A. You'd ssh to shell.uoregon.edu

Password

Q. How/where do I change my password for my uoregon.edu account?

A. Go to **https://password.uoregon.edu/** After you change your password, please allow 15-30 minutes for your new password to be fully activated.

Mailing Lists

Q. What happens to mailing lists on lists.uoregon.edu?

A. They continue to be served from lists.uoregon.edu.

Q. What name should I use when transferring files to my uoregon.edu account via FTP?

A. You should not use FTP. FTP exposes your password to sniffing (network interception). Use SCP or SFTP instead (common clients are SSH Secure Shell File Transfer client and Fugu).When using SCP or SFTP, you should connect to shell.uoregon.edu

More Questions?

Please contact Joe St Sauver (*joe@uoregon.edu*).

What Are Those Little RSS or XML Tags On

Joe St Sauver, Ph.D.
Director, User Services and Network Applications
joe@uoregon.edu

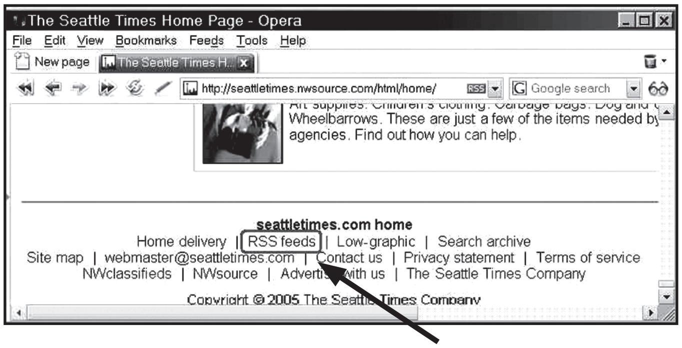
When you visit news sites or similar types of information sites these days, you may notice small "RSS" or "XML" links on those pages. Some examples of major online websites that have RSS or XML links on their web pages include:

- *The BBC* (**http://www.bbc.co.uk/**)
- *Google News* (**http://news.google.com/**)
- *The New York Times* (**http://www.nytimes.com/**)
- *Slashdot* (**http://slashdot.org/**)
- *Wired News* (**http://www.wired.com/**)
- *Yahoo! News* (**http://news.yahoo.com/**)

There are many others, although you may sometimes need to dig around to find the RSS or XML link on the page. More often than not, however, RSS or XML links are included on major news sites.[1]

Unfortunately, if you try clicking on one of those links in many popular web browsers, you'll often see only an ugly page of text that looks like gibberish, containing lots of raw XML code. If this happens to you, the problem is that you're using the wrong tool. Most web browsers do not know how to properly interpret RSS feeds "out of the box." While you could get around that problem by using a specialized RSS news aggregator program or by adding an RSS plug-in to your current web browser, one solution that works really well for reading RSS feeds is to use the free web browser Opera, which *does* know how to handle RSS without any modification. If you don't currently have Opera on your system, you can download it for free from **http://www.opera.com/**

Once you have installed Opera, find a website that has an RSS feed. For example, the *Seattle Times* newspaper has an RSS feed link tucked away at the bottom of **http://seattletimes.nwsource.com/html/home/**


The Seattle Times Home Page - Opera
File Edit View Bookmarks Feeds Tools Help
New page
The Seattle Times H...
http://seattletimes.nwsource.com/html/home/
RSS
Google search

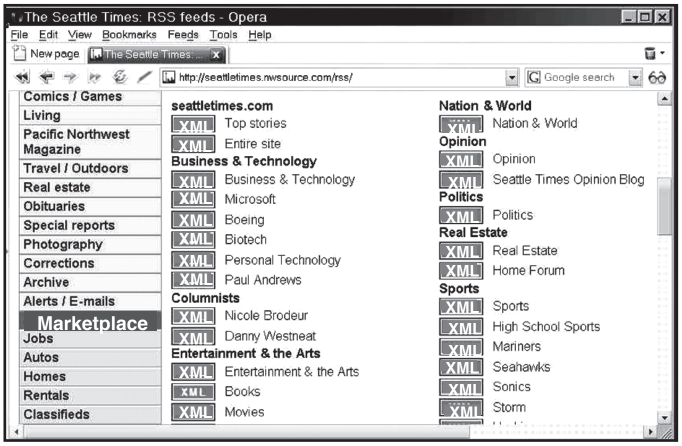
Art supplies. Children's clothing. Garbage bags. Dog and
Wheelbarrows. These are just a few of the items needed by
agencies. Find out how you can help.

seattletimes.com home
Home delivery | RSS feeds | Low-graphic | Search archive
Site map | webmaster@seattletimes.com | Contact us | Privacy statement | Terms of service
NWclassifieds | NWsource | Advertise with us | The Seattle Times Company

Copyright © 2005 The Seattle Times Company

The Seattle Times online, with RSS feeds link selected.

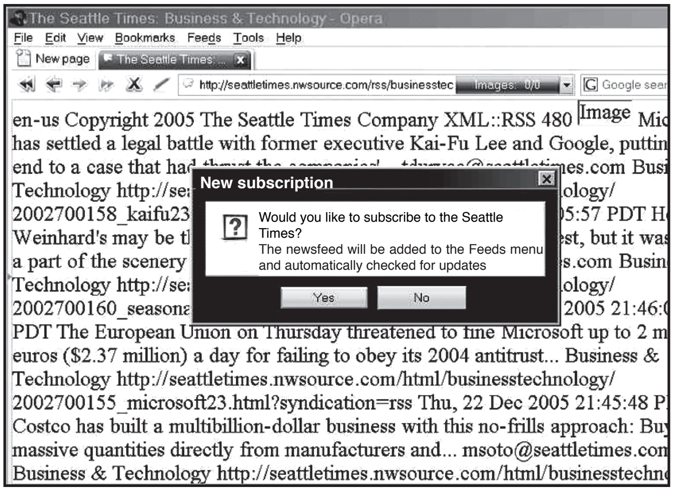
If you click that link, you'll be taken to a page full of XML links representing various parts of the Seattle Times site:



seattletimes.com
XML Top stories
XML Entire site
Business & Technology
XML Business & Technology
XML Microsoft
XML Boeing
XML Biotech
XML Personal Technology
XML Paul Andrews
Columnists
XML Nicole Brodeur
XML Danny Westneat
Entertainment & the Arts
XML Entertainment & the Arts
XML Books
XML Movies

Nation & World
XML Nation & World
Opinion
XML Opinion
XML Seattle Times Opinion Blog
Politics
XML Politics
Real Estate
XML Real Estate
XML Home Forum
Sports
XML Sports
XML High School Sports
XML Mariners
XML Seahawks
XML Sonics
XML Storm

You could pick any of those sections, but for this example let's choose Business and Technology. When we click on that link, we see:

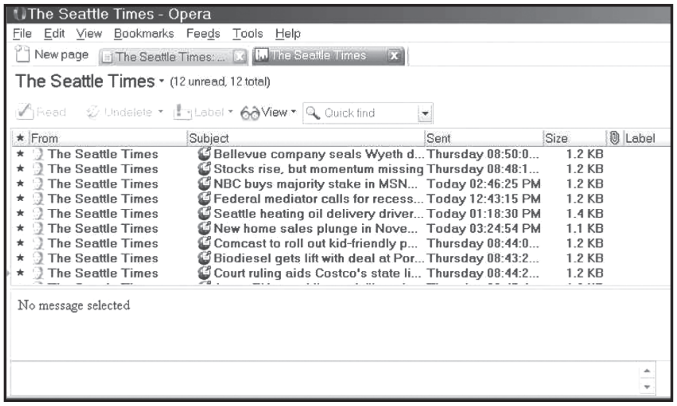

The Seattle Times: Business & Technology - Opera
File Edit View Bookmarks Feeds Tools Help
New page
The Seattle Times: ...
http://seattletimes.nwsource.com/rss/businesstec
Images: 0/0
Google sear
Image
Yes
No

en-us Copyright 2005 The Seattle Times Company XML::RSS 480 Mic
has settled a legal battle with former executive Kai-Fu Lee and Google, puttin
end to a case that ha ... es.com Busi
Technology http://se ... ology/
2002700158_kaifu23 ... 05:57 PDT H
Weinhard's may be t ... est, but it was
a part of the scenery ... s.com Busin
Technology http://se ... ology/
2002700160_seasona ... 2005 21:46:
PDT The European Union on Thursday threatened to fine Microsoft up to 2 m
euros ($2.37 million) a day for failing to obey its 2004 antitrust... Business &
Technology http://seattletimes.nwsource.com/html/businesstechnology/
2002700155_microsoft23.html?syndication=rss Thu, 22 Dec 2005 21:45:48 P
Costco has built a multibillion-dollar business with this no-frills approach: Bu
massive quantities directly from manufacturers and... msoto@seattletimes.com
Business & Technology http://seattletimes.nwsource.com/html/businesstechn

New subscription

Would you like to subscribe to the Seattle Times?
The newsfeed will be added to the Feeds menu and automatically checked for updates

When you click Yes to subscribe to that feed, you'll then see:



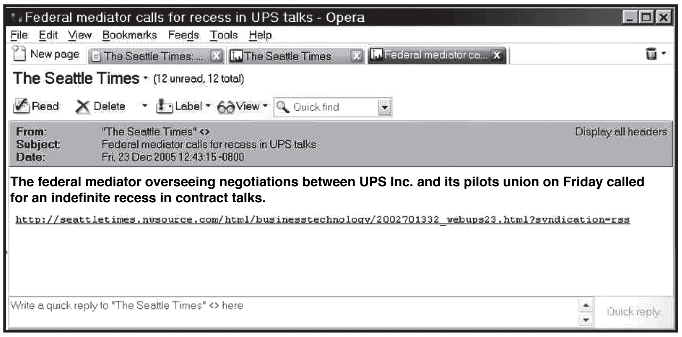
The Seattle Times (12 unread, 12 total)

★	From	Subject	Sent	Size	Label
★	The Seattle Times	Bellevue company seals Wyeth d...	Thursday 08:50:0...	1.2 KB	
★	The Seattle Times	Stocks rise, but momentum missing	Thursday 08:48:1...	1.2 KB	
★	The Seattle Times	NBC buys majority stake in MSN...	Today 02:46:25 PM	1.2 KB	
★	The Seattle Times	Federal mediator calls for recess...	Today 12:43:15 PM	1.2 KB	
★	The Seattle Times	Seattle heating oil delivery driver...	Today 01:18:30 PM	1.4 KB	
★	The Seattle Times	New home sales plunge in Nove...	Today 03:24:54 PM	1.1 KB	
★	The Seattle Times	Comcast to roll out kid-friendly p...	Thursday 08:44:0...	1.2 KB	
★	The Seattle Times	Biodiesel gets lift with deal at Por...	Thursday 08:43:2...	1.2 KB	
★	The Seattle Times	Court ruling aids Costco's state li...	Thursday 08:44:2...	1.2 KB	

No message selected

Web Pages?

Double-click on one of the listed articles to see it. For example:


Federal mediator calls for recess in UPS talks - Opera
File Edit View Bookmarks Feeds Tools Help
New page
The Seattle Times: ...
The Seattle Times
Federal mediator ca...
The Seattle Times (12 unread, 12 total)
Read
Delete
Label
View
Quick find
Display all headers
Quick reply

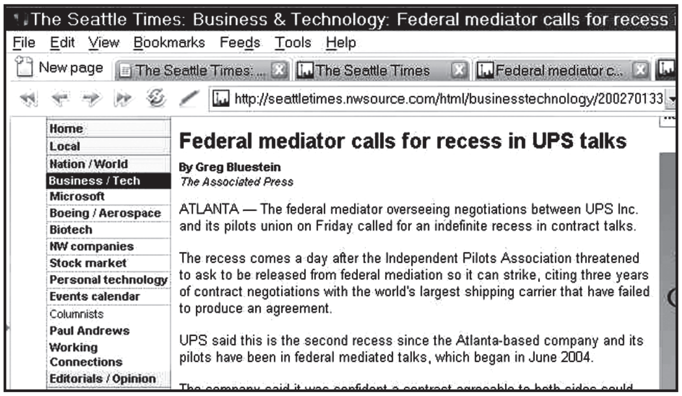
From: "The Seattle Times" <>
Subject: Federal mediator calls for recess in UPS talks
Date: Fri, 23 Dec 2005 12:43:15 -0800

The federal mediator overseeing negotiations between UPS Inc. and its pilots union on Friday called for an indefinite recess in contract talks.

http://seattletimes.nwsource.com/html/businesstechnology/2002701332_webups23.html?syndication=rss

Write a quick reply to "The Seattle Times" <> here

If the brief synopsis of the article looks interesting, click on the link to retrieve the whole article:



Federal mediator calls for recess in UPS talks

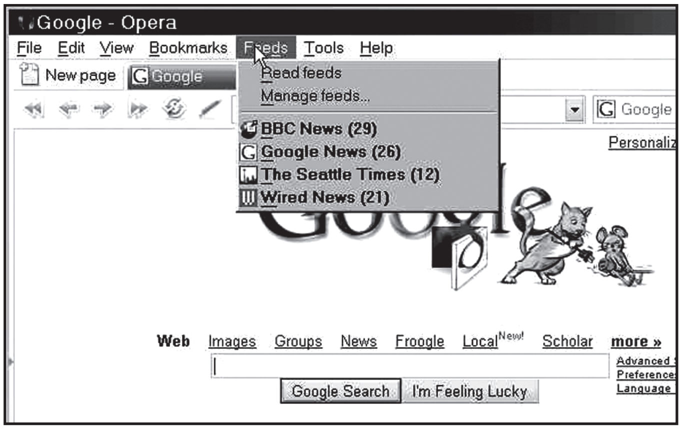
By Greg Bluestein
The Associated Press

ATLANTA — The federal mediator overseeing negotiations between UPS Inc. and its pilots union on Friday called for an indefinite recess in contract talks.

The recess comes a day after the Independent Pilots Association threatened to ask to be released from federal mediation so it can strike, citing three years of contract negotiations with the world's largest shipping carrier that have failed to produce an agreement.

UPS said this is the second recess since the Atlanta-based company and its pilots have been in federal mediated talks, which began in June 2004.

When you're ready to go back and check out your other RSS feeds, go to Opera's Feeds menu and pick another feed to visit:



or just go to "Read Feeds" to check what's new from ALL your RSS feeds.

Why Would I Want to Subscribe to RSS Feeds?

The real value in RSS feeds lies in RSS's ability to easily check and interleave multiple RSS feed sources on an automated basis.

Once you've subscribed to feeds of interest, you can quickly scan new items, selecting only the ones that look interesting and skipping the rest.

RSS represents pure content, with none of the encrusted blinking advertising and miscellaneous cruft that you'd otherwise have to wade through just to look for updated news items. Moreover, most RSS readers keep track of what you've already read, so you don't need to remember what you've seen and what you haven't—your RSS reader will do it for you. You can concentrate solely on the new content that's available.

Some sites, such as *Yahoo News*, will even let you create custom RSS feeds. For example, if you're attending the UO from Fiji and want an exclusive RSS feed of *Yahoo News* items about Fiji, *Yahoo News* will let you build a custom RSS feed to satisfy that specific desire.

Don't Get Carried Away

RSS feeds actively pull content from RSS feed sites. Because of that, if some enthusiastic RSS users subscribe wantonly, setting their systems to frequently poll a large number of sites for new RSS items on a rapid basis, the load on those RSS feed sites can quickly become substantial. Please show restraint, and "only take what you can eat."

In particular, please try to live with the default three-hour polling interval that Opera uses when retrieving RSS subscription content if at all possible.

Also, if you're no longer interested in a particular RSS feed that you once subscribed to, please delete it from the feeds you routinely check—don't let it run forever.

Questions?

UO faculty, UO students or UO staff with questions about reading RSS feeds with Opera are welcome to contact me at *joe@uoregon.edu*

Notes:

[1] I've begun maintaining a list of major sites offering RSS feeds at **http://www.uoregon.edu/~joe/rss.html** If there are major sites I've missed, or sites of special relevance to Oregon, feel free to suggest them to me (all suggestions are subject to acceptance).

Internet Milestone: One Billion Users!

In his December 19 *Alertbox* report, Jacob Nielson noted that Internet users reached the one-billion mark in 2005. That number is expected to double in the next ten years. For more details, see

http://www.useit.com/alertbox/internet_growth.html

Virtual Private Network (VPN) Service Adds Web Access

Now you can create a VPN connection using a standard web browser

Patrick Chinn
Distributed Network Computing Consultant
pchinn@uoregon.edu

The Computing Center recently expanded its Virtual Private Network (VPN) service with the addition of WebVPN.

WebVPN allows you to create a VPN connection to UOnet, the university's network, using a standard web browser. It does not require the installation of any additional software. Since it does not require any extra software, WebVPN will simplify the process required to connect from off-campus to restricted resources on the web.

When do you need it? WebVPN is best suited for situations when you need to access websites that are restricted to UOnet users only. Since WebVPN creates a connection for only one web browser window, it is not appropriate for use with other programs that connect to the Internet (such as email programs like Thunderbird).

How do you use it? To use WebVPN, open a web browser to **https://uo-vpn3-gw.uoregon.edu/** To connect, enter your uoregon.edu email address and password, and click the Login button. If the connection is successful, you will see a "Welcome to the University of Oregon Virtual Private Network" message. Click the OK button to continue.

Your WebVPN connection to UOnet consists of this single web browser window. How can you tell that you're connected using WebVPN? Look for the white-on-teal toolbar in the upper right corner of the browser window (see Fig. 1 below). This toolbar is a key element in WebVPN. It indicates that you are connecting using VPN and it provides access to frequently-used features.

VPN toolbar

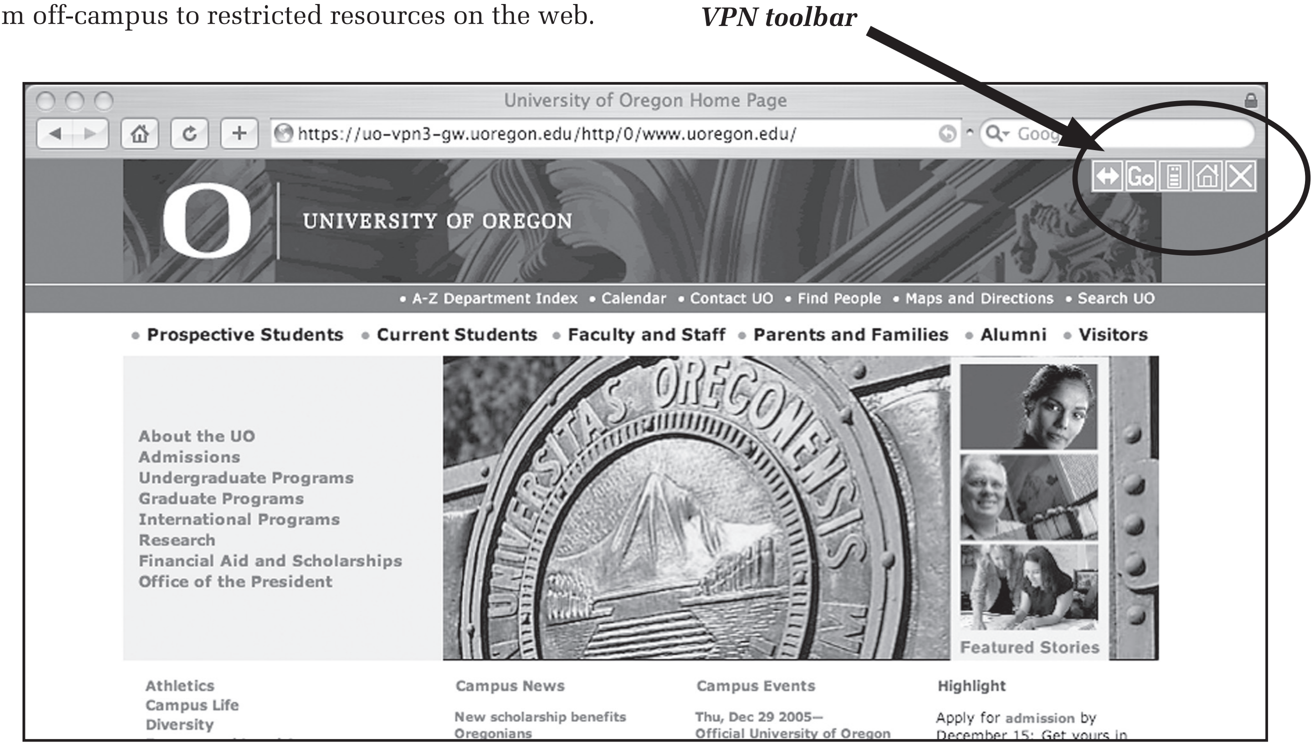
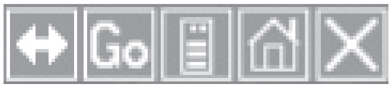

University of Oregon Home Page
https://uo-vpn3-gw.uoregon.edu/http/0/www.uoregon.edu/
Goog
Go
UNIVERSITY OF OREGON
• A-Z Department Index • Calendar • Contact UO • Find People • Maps and Directions • Search UO
• Prospective Students • Current Students • Faculty and Staff • Parents and Families • Alumni • Visitors
About the UO
Admissions
Undergraduate Programs
Graduate Programs
International Programs
Research
Financial Aid and Scholarships
Office of the President
UNIVERSITAS OREGONENSIS
Featured Stories
Athletics
Campus Life
Diversity
Campus News
New scholarship benefits Oregonians
Campus Events
Thu, Dec 29 2005—
Official University of Oregon
Highlight
Apply for admission by December 15: Get yours in

Fig. 1: The WebVPN connection page, which opens after you successfully log in.

The buttons on the VPN toolbar are (from left to right): double arrow, Go, Computer, Home and X:



The double arrow button moves the toolbar from the right side of the web page to the left, or vice versa. Use this button if the toolbar obscures part of the web page you wish to view.

Use the Go button when you wish to enter the address of a web page you'd like to visit.

Opening the advanced toolbar. The Computer button (shown circled below) opens the WebVPN advanced toolbar:

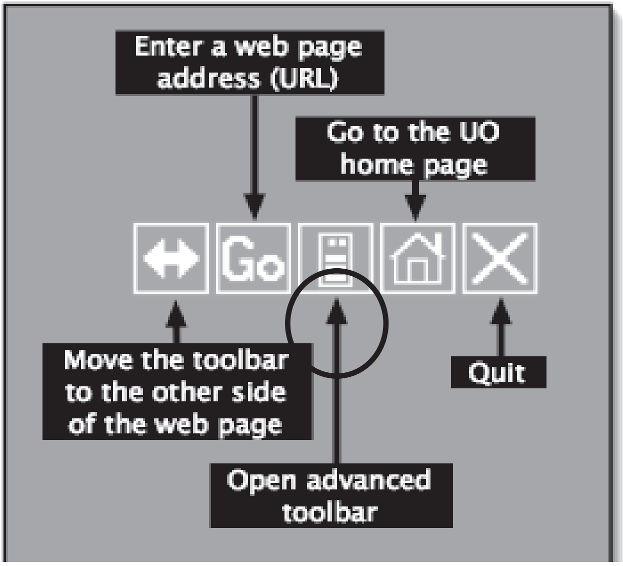

Enter a web page address (URL)
Go to the UO home page
Go
Move the toolbar to the other side of the web page
Quit
Open advanced toolbar

Fig. 2: The WebVPN toolbar functions, with the Computer button circled. Clicking the Computer button opens the advanced toolbar.

The functions of the advanced toolbar are beyond the scope of this article, but you may learn more about how to use them by going to **http://micro.uoregon.edu/getconnected/webvpn.html**

Accessing specific websites. There are two preferred ways to access specific websites. Suppose you want to view the Image Reserves on the Library's website (**http://libweb.uoregon.edu/**). The first way to get there is to click the Libraries link on the main UO web page, which loads when you log in. The second method is to click the Go button in the WebVPN toolbar and then type the address of the page you wish to visit.

Accessing the main UO web page. Clicking the Home button will take you to the main UO web page.

Logging out. The X button is used to end your WebVPN session. To log out of WebVPN, click the X button.

One word of caution: it is easy to inadvertently close your WebVPN session without meaning to. Two common ways of unintentionally terminating your WebVPN connection are:

- selecting a bookmarked website in your web browser
- clearing the web page address (URL) and typing a new one

'Classic' Non-web VPN Also Available

If you prefer, you may use the original, "classic" way of making a VPN connection to UOnet (see VPN links at **http://micro.uoregon.edu/getconnected/**)

More Information

For more general information on VPN, see **http://micro.uoregon.edu/getconnected/vpn_overview.html**

Industry News

Cyrusoft Files for Bankruptcy

On November 18 Cyrusoft International, Inc., announced it was going out of business and filed for Chapter 7 bankruptcy. Cyrusoft is the author of the Mulberry email client, a favorite of some UO users. For details, see

http://cyrusoft.com/

Silicon Graphics Dropped by NYSE

Silicon Graphics, once a leader in supercomputing and graphics software development, was dropped from the New York Stock Exchange on November 7 after its stock price dipped below the minimum standard for NYSE listings. For details, see

http://slashdot.org/articles/05/11/03/1325203.shtml?tid=139&tid=187&tid=98

http://www.sgi.com/company_info/newsroom/press_releases/2005/november/nyse.html

Blackboard Merges with WebCT

On October 12 Blackboard and WebCT, both major providers of education enterprise software and services, announced plans to merge. The company will remain under the Blackboard brand. For answers to frequently asked questions about how the merger will affect clients, see WebCT's FAQs page at

http://hub-images.webct.com/resources/sinatra/mergerArticle.html

For more details about the business consequences of the merger, see **http://www.blackboard.com/WebCT**

BlackBerry Maker Loses Supreme Court Appeal

Research in Motion Ltd (RIM), the makers of the popular BlackBerry handheld email device, lost the first round of its appeal of a patent infringement case in October, and now faces a court order that may shut down its operations in the U.S.

Rival company NTP, which brought the patent suit against RIM, has already benefited from the litigation by selling licenses to BlackBerry rivals, including Nokia and Good Technology. For details, see

http://www.bloomberg.com/apps/news?pid=10000082&sid=aXg_WxvhN.go&refer=canada

http://www.businessweek.com/technology/content/dec2005/tc20051215_806425.htm

If Your Needs Are Simple, OpenOffice 2.0 Is

This Open Source program incorporates most of the functionality of the Microsoft Office suite…and it's free!

Spencer Smith
Microcomputer Support Specialist
spencera@uoregon.edu

Microsoft Office has been the de facto standard for word processing, spreadsheets, and business presentations for many years. Because of the pervasive use of the Microsoft suite of programs, many students and faculty purchased that suite by default. If your needs are simple, though, there may be an alternative: OpenOffice.

In collaboration with the open source community, Sun Microsystems has developed a productivity suite that is compatible with the Microsoft Office suite. OpenOffice (**http://www.openoffice.org/**) is freely available for download from the Internet. It incorporates most of the functionality of the Microsoft suite and is compatible with the file formats that Microsoft's products produce.

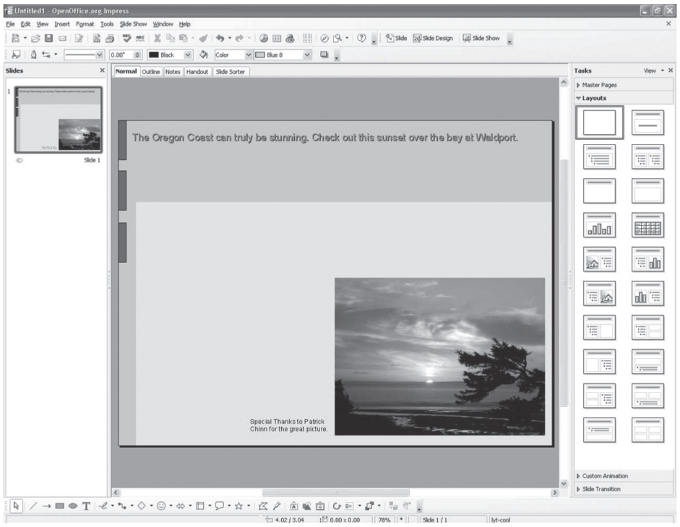
I need to stress the 'most' in 'most of the functionality.' OpenOffice's Writer module will open Microsoft Word documents and will save out in Microsoft .doc format (as well as Office 2003 .xml format.) However, document revision tracking, advanced document linking, and some other advanced functionality is lacking in OpenOffice Writer. It's a good basic word processor, without many of the frills and fillips that Microsoft has incorporated into Word.

The OpenOffice spreadsheet module, Calc, has similar benefits and limitations. It has all the basic functions and formulas available, and offers various printing and display formats for the finished product. Calc is also compatible with its Microsoft analog, Excel, and will open and save as Excel documents. Some of the more advanced features of Excel (for instance, changing the color of the tab at the top of a column) are missing or obscured in Calc. But the basic functionality is there, and Calc is as easy to use and learn as Excel.

All of the other modules have the same pretty-close-to-Microsoft feel to them. Impress, the presentation module, has the standard set of text, drawing, and media-import tools available. Draw is a basic vector-based* drawing program, similar to (but more limited than) Adobe Illustrator. The Base module implements a fundamental database, with tables, forms, queries and reports similar to Access. The Math module has mechanisms for creating and displaying complex mathematical formulas.

All the modules are relatively clean, with a clear, easy-to-understand interface. With a little patience and willingness to explore, a new user can be up and running in a very short time. People with years of experience in Microsoft's products may be frustrated by the subtle differences between the two offerings, but they should be able to bang out a paper or format a simple spreadsheet without any significant problems.

To give you an idea of the interface, a couple of sample OpenOffice windows are shown in Figures 1 and 2 below.



The Oregon Coast can truly be stunning. Check out this sunset over the bay at Waldport.

Special Thanks to Patrick Chinn for the great picture.

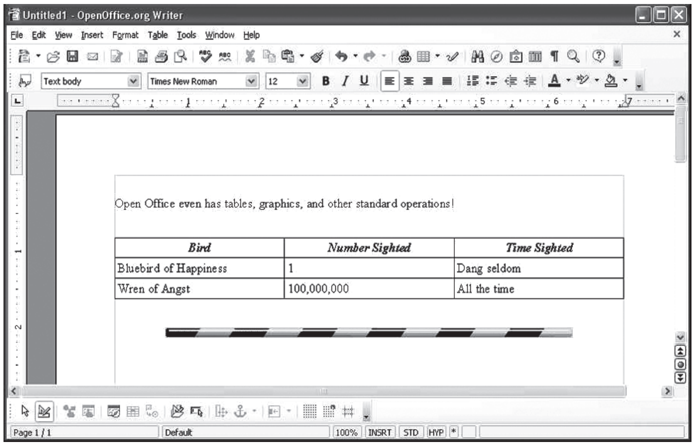
Fig. 1: Sample OpenOffice Impress (presentation module) window.

For the Macintosh, the analogous product suite (based on the same code and with the same limitations) is NeoOffice/J (**http://www.neooffice.org/**). There is usually some lag time between a feature in OpenOffice making its way into NeoOffice/J for the Mac; however, NeoOffice/J does a pretty good job of filling the need for a good,

Linux Kernel Finds a Home in Corvallis

Linux now lives in Oregon! The heart of Linux currently beats at Oregon State University's Open Source Lab. See **http://linux.slashdot.org/article.pl?sid=05/09/18/1348239&tid=106** for details.

An Attractive Alternative


Untitled1 - OpenOffice.org Writer
File Edit View Insert Format Table Tools Window Help
Text body
Times New Roman
12
Page 1 / 1
Default
100%
INSRT
STD
HYP

Open Office even has tables, graphics, and other standard operations!

Bird	Number Sighted	Time Sighted
Bluebird of Happiness	1	Dang seldom
Wren of Angst	100,000,000	All the time

Fig. 2: Sample OpenOffice Writer (word processor module) window.

free productivity suite on the Mac. NeoOffice/J lacks a database module, much like the analogous Macintosh Office suite from Microsoft; otherwise, OpenOffice and NeoOffice/J are essentially the same.

Open Source Caveats. The drawbacks to using OpenOffice or NeoOffice/J revolve around their nature as open source projects. They come with no warranty whatsoever, and although the documentation available through the 'Help' menu is pretty good, there is no '800' number to call for support. Online searches through Google or newsgroups may yield more results, but problems are mainly left as an exercise for the end user.

OpenOffice is a freely available and fast productivity suite. But if you need the warranty, support, and full application compliance, you may prefer to pay for the full Microsoft product instead.

OpenOffice Available on UO Public Domain Servers. For the convenience of UO users, Microcomputer Services has made OpenOffice available on its public domain servers (see **http://micro.uoregon.edu/pd/** for details on how to access these servers).

If you're affiliated with a UO department and prefer to purchase the Microsoft Office Suite for campus use, please see the website for The Organization for Educational Technology and Curriculum (OETC) at **http://www.oetc.org/**

* A vector-based graphics program creates forms and shapes by calculating the outline, fill, and curve characteristics mathematically, composing all the resulting shapes and forms into a series of equations that describe the scene. In contrast, a bitmapped graphics program treats each individual point or pixel on the screen discretely, manipulating the color values of each point individually.

what's new in the docs room?

Build Your Skills with Workshops-to-Go

Vickie Nelson
Documents Room Librarian
vmn@uoregon.edu

If you're new to Mac OS X or Photoshop, or are an old hand interested in taking your skills to the next level, come check out some of the new training CDs and DVDs in the Documents Room Library.

Mac Academy's five-disk *Mac OS X Tige*r offers 12 hours of training, including installation, preferences, and toolbar customization. You'll also get good introductions to Exposé, Dashboard, Spotlight, iCal, the Safari browser, and other nifty Mac features.

KW Computer Training's *Photoshop CS2 for Beginners* features Certified Adobe instructor Dave Cross introducing the tools you need to get up and running. In this two-hour workshop you'll learn to use floating palettes, layers, and filters, and find out how to crop and retouch your images.

Photoshop users who are past the beginner stage can reach the next level with Photoshop guru Scott Kelby's *Photoshop CS2 Power Session*. On this two-hour DVD, Kelby delves deeper into features for digital photographers, and introduces two new features: the Adobe Bridge and the Camera Raw plug-in.

The Documents Room also has many other instructional CDs, DVDs, and VHS tapes on a wide range of computing topics. All training disks circulate for one week and are renewable.

Call **346-4406** for more information, or visit the Documents Room website at **http://docsrm.uoregon.edu/**

Sober-Y Virus Doubles Number of Rejected

Joe St Sauver, Ph.D.
Director, User Services and Network Applications
joe@uoregon.edu

You may know that the Computing Center has been battling email spam, viruses, phishing, and other unwanted email traffic for many years now. We've primarily focused on blocking unwanted email originating from known spam sources, as well as unwanted email originating from compromised broadband-connected consumer systems acting as "spam zombies." [1]

What you may *not* know is just how hard the bad guys have been hammering the UO's email servers, or how rapidly the general worldwide email environment has deteriorated over the last month or so.

Specifically, the number of rejected inbound email connections on the main uoregon.edu SMTP servers has skyrocketed from under 200,000/day to over 450,000/day (see the graph on the following page). That's a tremendous increase to have occurred literally overnight. As you look at the graph, please note:

1) The graph shows rejected email *connections*, not rejected email *messages*. Each connection may represent one blocked email, or a hundred or a thousand or more—there's no way to know for sure without first accepting *all* inbound messages, good or bad, and then (and only then) categorizing each message as wanted or unwanted.[2]
2) In some cases, there may be tens of thousands of rejected connections, all associated with a single system that refuses to take "no" for an answer. Just as one example of this, consider rejected connections associated with the host 234.157.204.68.cfl.res.rr.com [68.204.157.234]:

Date	Rejected Connections
December 15, 2005	6,377
December 16, 2005	22,214
December 17, 2005	22,153
December 18, 2005	23,181
December 19, 2005	23,458
December 20, 2005	23,058
December 21, 2005	22,029
December 22, 2005	22,326

While a dozen systems running that hot could account for the doubling in rejected connections we're currently seeing, most connecting hosts do *not* repeatedly connect tens of thousands of times the way this example has been doing.

3) The graph included with this article covers all types of rejected inbound email connections, including conventional spam, viral messages, phishing/fraudulent email messages—and yes, even inadvertently blocked legitimate email.

That said, do we know (or at least think we know) what's been causing the huge increase? The answer is yes. While there were over 17,000 new viruses or virus variants in 2005, we believe that the jump in unwanted connections we're seeing is almost entirely associated with a single new virus: Sober-Y.[3]

In case you can't keep your viruses straight without a scorecard, Sober-Y is the mass mailing worm that emerged in earnest around Thanksgiving, which corresponds nicely with the jump in rejected connections shown in our graph. Sober-Y sends infectious email messages purporting to be from the FBI, from the CIA, or in the case of German language versions, from the German Bundeskriminalamt (BKA). The body of the English-language Sober-Y message usually claims to have "logged your IP address on more than 30 illegal Websites. Please answer our questions!" Of course, no such logging has in fact taken place, the message was not from the FBI [4], the CIA, or any other federal agency, and if you opened the enclosed attachment your system would become infected and the process would iterate. (Other less commonly seen variants of the virus claimed to include a Paris Hilton video as an attachment, or to be a registration confirmation.)

Here at the UO, from a user's point of view, Sober-Y was largely a non-event. Many of our users didn't even know that Sober-Y was in circulation. The antivirus filtering on uoregon.edu[5] did a great job of preventing Sober-Y from reaching user mailboxes, and copies obtained by UO users via departmental mail servers or other third-party email systems were well blocked by McAfee on the desktop (McAfee had definitions effective in blocking Sober-Y in distribution as of November 16). [6]

Unfortunately, there are systems elsewhere on the Internet that were not so well protected, and many of those systems were apparently compromised by this malware. Those compromised hosts continue to hammer away at SMTP servers all around the world, including ours. Postini, a major integrated message management service, declared Sober-Y to be the biggest virus outbreak it's ever processed—twice as large as the largest previous attack on record.[7] At least in some cases, Sober-Y is known to have resulted in email backlogs and delays,[8] although the UO's email servers have continued to function normally.

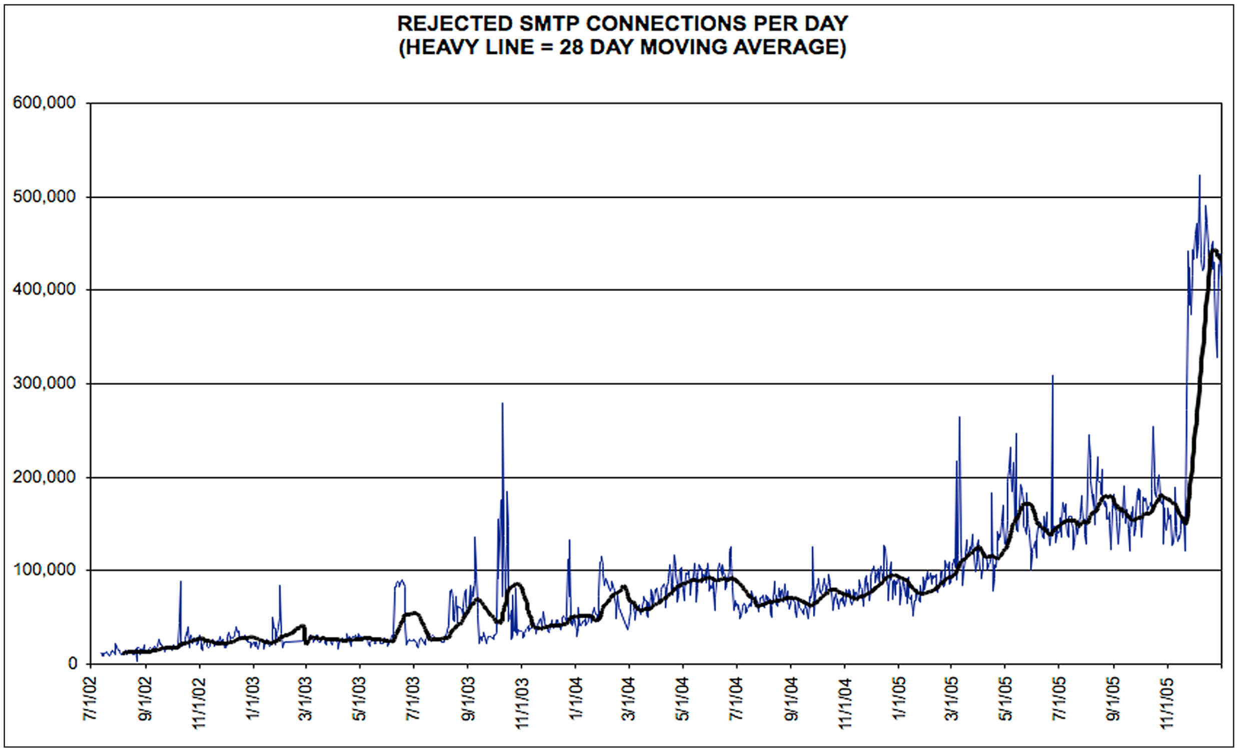
As mentioned in reference **[6]** at the conclusion of this article, Sober-Y is apparently scheduled to update itself on Friday January 6th. However, it remains to be seen if that update will be effective, given the success that antivirus vendors have had in cracking the scheme that Sober-Y had planned to employ.

In the meantime, we appreciate your patience as we deal with the panoply of online threats we collectively face each day. We know what a pain spam, viruses, worms, and all the other types of unwanted online traffic can be, and we're working hard to keep all of it from affecting your work online.

SMTP Connections During December 2005

If at any time you want to opt out of the UO's default spam filter (or if you've opted out and think you might want to opt back in), you can do so by using the interactive form online at **http://password.uoregon.edu/allowspam/**

Questions, comments, concerns? If you're a UO faculty member, a UO student, or a UO staff person and have any questions about Sober-Y or virus and spam filtering at the UO, feel free to contact me (*joe@uoregon.edu* or **346-1720**).



Notes:

[1] For more information on spam zombies, please see
http://www.uoregon.edu/~joe/zombies.pdf
http://www.ftc.gov/bcp/conline/edcams/spam/zombie/

[2] Unfortunately, it simply isn't practical for us to initially accept all inbound messages, regardless of whether they're good or bad, for several reasons:

- If you don't reject unwanted messages at connect time (e.g., while the remote server is still connected to our mail server), there's a real problem when messages you've initially accepted subsequently turn out to be spam, or to be otherwise unwanted. Why? If you initially indicate that you're accepting a message, telling the remote transferring system that you're going to do so, you really should deliver the message—unless you subsequently notify the sender that you won't be doing so.
- Virtually all viral email and spam email has a forged apparent sender address (also known as a faked "From:" or a faked "Reply-To:" header), usually the name of some innocent person.
- Because the remote server is no longer connected (it disconnected after you accepted the message) and because the apparent sender address is untrustworthy, you have no effective way of reporting that you've got a message that you *said* you were going to deliver but which in fact you really can't.

You now understand why we strive to reject virtually all messages at connect time: if a message cannot be delivered, the remote server immediately gets the bad news while it is still connected, thereby allowing it to alert the sender to the nondelivery of their message.

- The other reason why it really isn't practical to initially accept all incoming mail, regardless of whether it is good or bad, relates to the relative volume of bad-to-good email right now. Currently, depending on who you listen to and how you define unwanted email, between two-in-three and nine-in-ten incoming email messages are unwanted. To handle all that ultimately unwanted email, your email server's capacity would have to be increased nearly tenfold, just to accept mail you'll ultimately discard. That's a tremendous expense and a real waste of disk space, bandwidth, CPU time, etc.

[3] For more information on Sober-Y, see **http://secunia.com/virus_information/23836/sober.x/** (Note that due to a lack of coordination among antivirus vendors, some refer to this virus as Sober-Y, while others refer to it as Sober-X)

[4] The official disclaimer notices can be seen at
http://www.fbi.gov/page2/nov05/emailscam112205.htm
http://www.cia.gov/cia/alerts.html
http://www.bka.de/pressemitteilungen/2005/pm211105.html (in German)

[5] **http://www.clamav.net/**

[6] **http://vil.nai.com/vil/content/v_137072.htm**

[7] **http://www.postini.com/news_events/pr/pr112905.php**

[8] **http://www.washingtonpost.com/wp-dyn/content/article/2005/12/07/AR2005120702471.html**

« cybercrime in the news »

Spam Wars Continue

International Spam Ring Shut Down, Fined $37 Million Massachusetts prosecutors are still seeking Leo Kuvayev, the leader of the "Internet Spam Gang," whose operation managed dozens of illegal websites and sent out millions of messages peddling everything from counterfeit pharmaceuticals and pirated software to phony mortgage deals and pornography. Kuvayev and some of his cohorts are believed to be in Russia. For details, see **http://www.ago.state.ma.us/sp.cfm?pageid=986&id=1502**

419 Scammers Face Jail
Nigerian officials continue their campaign to eradicate the criminal Internet scams for which their country has become notorious. Several major spammers have already been apprehended and given stiff sentences for their role in bringing down the Banco Noroeste in Brazil with an elaborate advance-fee scam:
http://management.silicon.com/government/0,39024852,39154412,00.htm

http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/1/hi/world/africa/4690031.stm

'I Will Eat Your Dollars'
For an enlightening behind-the-scenes look at how 419 scams are perpetrated, see the *L.A. Times* article, "I Will Eat Your Dollars" at
http://www.latimes.com/technology/la-fg-scammers20oct20,0,301315.story?collection=la-yahoostorylinks

New California Law Cracks Down on Phishing

On October 1, Governor Schwarzenneger signed the nation's first law imposing stiff penalties on "phishers" (email con artists posing as legitimate businesses who trick victims into revealing sensitive personal information that can be used in ID theft). For details, see
http://www.msnbc.msn.com/id/9547692/

ID Theft

Feds Nab Major ID Thieves in Sting Operation. In November, six people who were involved in Internet sales of credit card, debit card, and PIN numbers, as well as other stolen identity information, pled guilty to fraud charges brought by the U.S. Secret Service. For details, see
http://www.wired.com/news/infostructure/0,1377,69616,00.html

Portland Drug Raid Uncovers ID Theft. Sensitive information that could be used in ID theft scams was found on a computer at the site of a recent drug raid in Portland, Oregon. Hundreds of thousands of names, birth dates, home addresses, Social Security numbers, and credit scores were among the data. Portland police are warning people to check their bank accounts and credit scores as a precautionary measure. See
http://www.portlandtribune.com/archview.cgi?id=32555

Botnet Crimes Become Big Business

California Botmaster Arrested. A recent California case involving a "botmaster" who employed armies of "zombie" computers to commit fraud exposes a new criminal trend in hacking. Employing a malicious program called a "bot," botmasters are able to hack into computers and harness their collective power for their own ends. In November, FBI agents arrested the most nefarious botmaster to date: a 20-year-old California man who ran a network of 400,000 compromised computers for illegal gain. For details, see
http://www.eweek.com/article2/0,1895,1881621,00.asp

Oregon Man Pleads Guilty in Botnet Crime. A 21-year-old Beaverton man recently pled guilty to launching DDoS attacks on the name server for Ebay.com via a botnet worm program. See
http://www.axcessnews.com/modules/wfsection/article.php?articleid=7363

Safety Alert: HP, Dell Recall Notebook Battery Packs

HP Notebook Battery Recall

In late October Hewlett Packard announced a recall and replacement program for approximately 125,00 battery packs used in certain HP notebooks shipped between March 2004 and September 2005. These batteries pose a potential hazard to users. The recall is for the batteries only, not the notebooks themselves. For complete information, including a list of all the affected notebooks, see
http://bpr.hpordercenter.com/bpr/

Dell Battery Pack Replacement Program

In late December, Dell issued a security recall for certain notebook batteries that were sold for use with some models of its Latitude, Precision, and Inspiron notebook computers. It is possible for these batteries to overheat, posing the risk of fire.

Complete details about the affected models and batteries are available at Dell's Battery Pack Recall Program website: **https://www.dellbatteryprogram.com/Default.aspx**

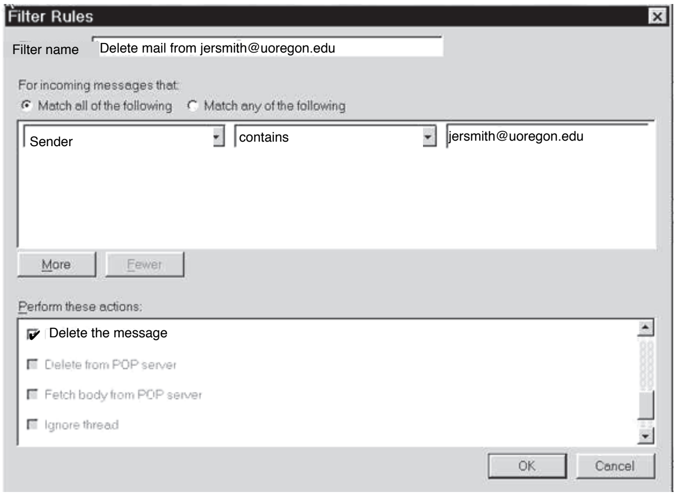
Client-Side Spam Filtering

While all uoregon.edu email accounts are spam-filtered by default[1], and that filter catches most of the spam targeting uoregon.edu email accounts, some users may also be interested in additional or alternative spam filtering.[2]

One easy way to add additional spam protection for your email is through use of a so-called "client-side" spam filter. Unlike the server-side spam filters we run for you on the uoregon.edu mail servers, client-side spam filters run on your PC or Mac and are installed, configured, and administered by you. One example of a client-side spam filter is the filter that's integrated with Thunderbird, our recommended PC and Mac IMAP email client.[3] Thunderbird offers two types of filtering: simple manually configured filters, and Bayesian junk email filters.

Simple Manually Configured Filters

Simple manually configured filters are great if you have unwanted messages that have a consistent, easily identified characteristic (such as an unchanging sender address, or a *Subject:* line that consistently contains the same word or words). To create a manually configured filter, start Thunderbird and go to Tools—>Message Filters. A Filter Rules window will appear. Define a rule in the top of this window, then choose what you'd like to have happen to messages that match that rule in the bottom of the Filter Rules window. For example, assume you're getting unwanted mail from *jersmith@uoregon.edu* and you want to automatically delete all messages coming from that sender. You could set up a filter rule that looks like this:



Filter Rules

Filter name: Delete mail from jersmith@uoregon.edu

For incoming messages that:

● Match all of the following ○ Match any of the following

Sender | contains | jersmith@uoregon.edu

Perform these actions:

☑ Delete the message
☐ Delete from POP server
☐ Fetch body from POP server
☐ Ignore thread

While you can create as many rules as you want, most spammers don't use an easily filtered, unvarying *From:* address or consistent *Subject:* header. You need more potent medicine to deal with typical spam today.

Thunderbird's Bayesian Filtering

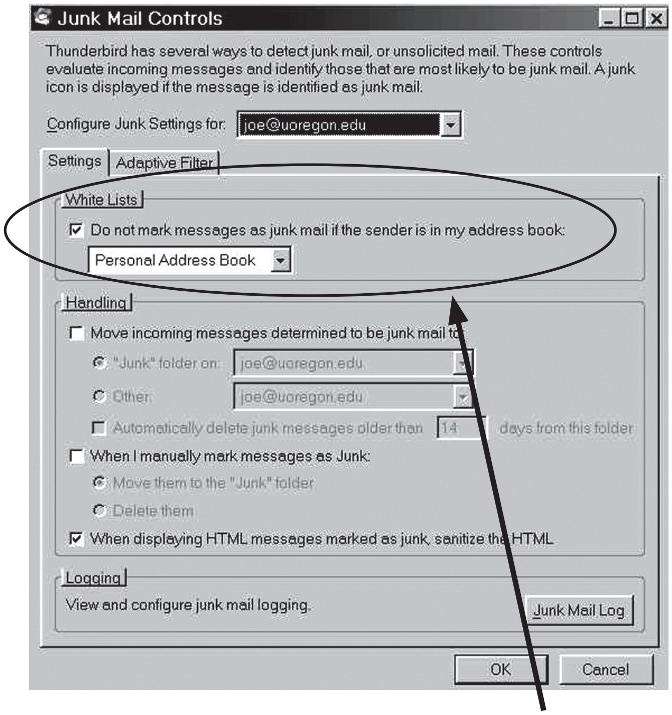
When you go beyond simple manually configured filters, Thunderbird relies on a content-oriented Bayesian approach[4] to spam filtering. This provides a nice complement to the UO's server-side spam filtering, which focuses on blocking known spam sources and spam from compromised end-user systems ("spam zombies.").

Bayesian spam filtering sorts messages into two categories: "spam" (unwanted junk mail) and "ham" (legitimate mail). Assigning messages to one group or the other is initially done manually by you, as part of the process of training the Bayesian filter. Once you've manually shown the filter what's ham and what's spam for awhile, you can then turn on automatic filtering and the spam filter will begin to categorize new messages based on the words that the filter has "seen" in your historical spam and legitimate mail messages.[5]

After a couple of weeks of initial training, the Bayesian filter will usually categorize correctly, but sometimes it may tag a real message as spam (a "false positive"), or it may still sometimes mistakenly allow unwanted messages (a so-called "false negative"). No filter is ever 100% free of false positives or false negatives, but I think you'll find that the Bayesian filter in Thunderbird does an excellent job of minimizing those errors.

Setting Up Client-side Filtering in Thunderbird

To access Thunderbird's built-in client-side spam filter, launch Thunderbird as you normally would. Then go to Tools—>Junk Mail Controls. You'll see a panel that looks like this:



Junk Mail Controls

Thunderbird has several ways to detect junk mail, or unsolicited mail. These controls evaluate incoming messages and identify those that are most likely to be junk mail. A junk icon is displayed if the message is identified as junk mail.

Configure Junk Settings for: joe@uoregon.edu

White Lists

☑ Do not mark messages as junk mail if the sender is in my address book:

Personal Address Book

Handling

☐ Move incoming messages determined to be junk mail to:

● "Junk" folder on: joe@uoregon.edu

○ Other: joe@uoregon.edu

☐ Automatically delete junk messages older than 14 days from this folder

☐ When I manually mark messages as Junk:

● Move them to the "Junk" folder

○ Delete them

☑ When displaying HTML messages marked as junk, sanitize the HTML

Logging

View and configure junk mail logging.

Begin by checking "Do not mark messages as junk mail if the sender is in my address book." By doing so, any messages that appear to come from a known correspondent (e.g., someone who's listed in your

- *continued on page 20*

Client-side Spam Filtering, continued…

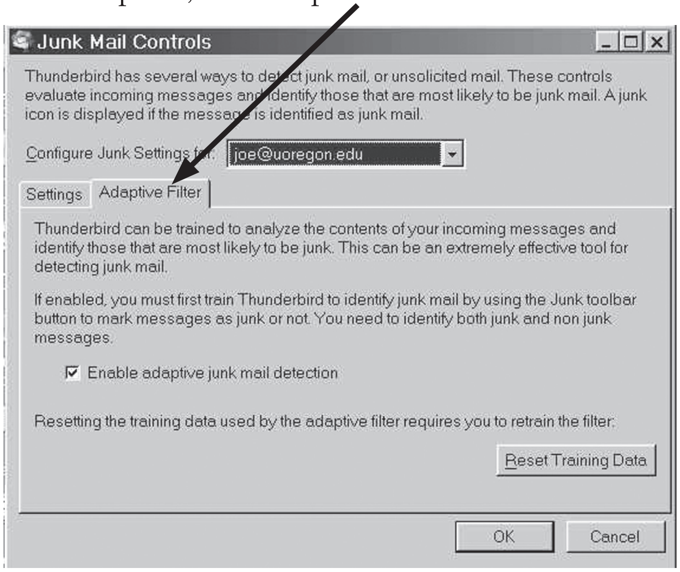
address book) will automatically be exempted from consideration as spam. This is a process usually known as "whitelisting."[6] If you plan to use Thunderbird's integrated junk mail filtering, you should be absolutely religious about whitelisting regular correspondents via your Thunderbird address book.

The next step is also key. Do *not* (yet) check "Move incoming messages determined to be junk mail." You'll want to first train your filter for a while by manually tagging stuff as junk, and reviewing what it tags as junk, before you trust the filter. *To repeat: do* **not** *(yet) check the "Move incoming messages determined to be junk mail" box!* Wait a few weeks while you train your filter, then come back and check that box if you want to.

Heads up about one other key setting on this panel: If you check the line beginning "Automatically delete junk messages older than 14 days from this folder," Thunderbird will also automatically delete messages that are at least two weeks old. If those messages are truly all junk, this is very convenient—and a good idea. Of course, if a *real* message accidentally gets mismarked, automatically deleting messages marked as junk means that you may unknowingly delete real mail messages unless you notice and "rescue" (unjunk) them in time.

Your next option concerns what happens to manually flagged junk mail. For now, set Thunderbird to move messages that have been manually flagged as junk to your Junk folder.

Another setting on that same panel is the "When displaying HTML messages marked as junk, sanitize the HTML." That box should also be selected for your protection. You're now ready to go to the other tab of the Junk Mail Controls panel, the "Adaptive Filter" tab:



Thunderbird has several ways to detect junk mail, or unsolicited mail. These controls evaluate incoming messages and identify those that are most likely to be junk mail. A junk icon is displayed if the message is identified as junk mail.

Configure Junk Settings for: joe@uoregon.edu

Thunderbird can be trained to analyze the contents of your incoming messages and identify those that are most likely to be junk. This can be an extremely effective tool for detecting junk mail.

If enabled, you must first train Thunderbird to identify junk mail by using the Junk toolbar button to mark messages as junk or not. You need to identify both junk and non junk messages.

☑ Enable adaptive junk mail detection

Resetting the training data used by the adaptive filter requires you to retrain the filter:

Check the "Enable adaptive junk mail detection" box on that tab, and then click OK.

Manually Flagging Spam In Thunderbird to Train the Bayesian Filter

The preliminaries out of the way, you're now ready to review your Inbox and manually flag any spam you find. By doing so, you'll be training your spam filter, essentially showing it examples of the sort of thing you don't want to receive in the future.

To flag messages as Junk, highlight one (or more) junk messages then click the Junk icon in the Thunderbird tool bar. If any good messages are erroneously marked as Junk, select them, then mark them as Not Junk by clicking on the Not Junk icon in the Thunderbird tool bar.

After you've trained the Bayesian filter for a few weeks, you can return to Tools—>Junk Mail Controls... and tell Thunderbird to begin automatically filing junk mail in the Junk folder.

What If I'm Using Outlook/Outlook Express?

Outlook and Outlook Express email clients also offer integrated spam filters similar to Thunderbird's. However, due to historical security issues with Outlook and Outlook Express,[7] we recommend that you consider migrating to our supported IMAP mail client, Thunderbird, instead.

What If I'm Using Thunderbird with POP?

POP (at least when used with large mailboxes) tends to be hard on the mail server, and POP doesn't work particularly well when you're filtering spam to a separate Junk folder (remember that as far as POP's concerned, it basically wants to deal with your default Inbox, and only your default Inbox). We urge you to use Thunderbird with IMAP rather than POP if you're planning to use Thunderbird's spam filtering features.

What If I'm Using UO Green or Blue Web Email?

Because you're not running Thunderbird on a PC or Mac when you're using the UO's green or blue Webmail, the Thunderbird-specific filtering options described in this article do not apply.

What If I Want to Use a *Commercial* Client-side Spam Filter?

If you like the idea of a client-side spam filter but you'd prefer a commercial client-side antispam filter, you may want to check out *PC Magazine*'s review of PC antispam products. See **http://www.pcmag.com/category2/0,1874,4795,00.asp** (you'll probably want to sort by editor rating by clicking on the up- and down-arrow in the editor rating column).

Questions?

If you're a UO faculty member, a UO student, or a UO staff person and have questions about client-side spam filtering, feel free to email Joe St Sauver at *joe@uoregon.edu*

Notes:

[1] Your uoregon.edu account is spam filtered unless you opt from the default spam filter by visiting **https://password.uoregon.edu/allowspam/**

[2] Another alternative to our default spam filtering is described in "Taking Control of Your Email…," **http://twin.uoregon.edu/~joelja/taking-email-control.html**

[3] If you don't have Thunderbird installed, you can download it from **http://www.mozilla.com/thunderbird/** For information about how to configure Thunderbird for use with your uoregon.edu account, see **http://micro.uoregon.edu/email/**

[4] Paul Graham's article, "A Plan for Spam," is a nice semi-technical introduction to Bayesian filtering (**http://www.paulgraham.com/spam.html**).

[5] Now you know why so many spam messages include text from online books or other seemingly random gibberish; the spammer's trying hard to avoid being blocked by Bayesian spam filters.

[6] Even if you whitelist particular correspondents by adding them to your Thunderbird address book, they may still be blocked by uoregon.edu's server-side spam filtering unless you opt out of the default server-side spam filtering as mentioned in note **[1]** above.

[7] See **http://www.sans.org/top20/#w4** or check **http://secunia.com/** for a list of vulnerabilities specific to the version of Outlook or Outlook Express that you're using.

« sites worth seeing »

1. **CALCONNECT.ORG, the Calendaring and Scheduling Consortium…**This informative site is devoted to developing interoperable standards for enterprise calendaring. Current participants include major U.S. universities (among them Stanford, MIT, Wisconsin, and UC Berkeley) and software vendors Oracle, Novell, the Mozilla Foundation, and others. **http://www.calconnect.org/**

2. **"Via Africa: Creating local and regional IXPs to save money and bandwidth"…** Using the successful deployment of a regional Internet Exchange Point (IXP) in Africa as an example, this document discusses the benefits of creating national and regional IXPs and explains how to create one. It was prepared for the 2004 Global Symposium for Regulators at the request of the International Development Research Centre (**http://network.idrc.ca/en/ev-1-201-1-DO_TOPIC.html**) and the International Telecommunication Union, and contains references to the work of the UO-based Network Startup Resource Center (**http://nsrc.org/**). **http://www.itu.int/ITU-D/treg/publications/AfricaIXPRep.pdf**

3. **Dual core processor information…**AnandTech's source for hardware analysis and news includes a discussion of dual core performance fixes. **http://forums.anandtech.com/messageview.aspx?catid=28&threadid=1707814&frmKeyword=&STARTPAGE=2&FTVAR_FORUMVIEWTMP=Linear**
   For a general overview of dual core CPUs, see **http://www.short-media.com/review.php?r=261**

4. **Enigmail: Thunderbird PGP Option for PC and Mac …**You may want to try Enigmail, an open-source Mozilla email client that offers encryption and authentication features. For details, see **http://enigmail.mozdev.org/**

5. **What's the Current State of Computer Network Security?…**The Computer Security Institute's annual report on information security, based on responses from 700 U.S. corporations, government agencies, financial and medical institutions, and universities. **http://www.gocsi.com/press/20050714.jhtml**

6. **Ajax information…** If you're looking for information on the Ajax (Asynchronous JavaScript and XML) web application, here are some useful sites:
   - "The Ten Best Ajax Links: Tutorials, Examples, and History" **http://www.mygadgetbag.com/MGBResearch/MGBResearchArticles/tabid/261/articleType/ArticleView/articleId/445/The-Ten-Best-Ajax-Links-Tutorials-Examples-and-History.aspx**
   - Articles:
     - "Ajax in Action": **http://books.slashdot.org/article.pl?sid=05/11/23/1426249&tid=6**
     - "Ajax (programming)": **http://en.wikipedia.org/wiki/AJAX**
     - "A Simpler Ajax Path": **http://www.onlamp.com/lpt/a/5841**

7. **Web developers' resource…** If you design or maintain a website, you may want to join lists. evolt.org, a site that hosts several mailing lists for web developers. Share your expertise and find answers to your own web-related questions. **http://lists.evolt.org/**

8. **"Sony's DRM Rootkit: The Real Story"…** Bruce Schneier looks behind the headlines on the recent brouhaha over Sony's copy-protection scheme **http://www.schneier.com/crypto-gram-0512.html#6**

Non-UO Recursive Domain Name Server Access

José Domínguez
Senior Network Engineer, Network Services
jad@network-services.uoregon.edu

Joe St Sauver, Ph.D.
Director, User Services and Network Applications
joe@uoregon.edu

Non-UO recursive access to the UO's DNS servers will be eliminated February 1.

Before explaining what this means, let's talk about who will ***not*** be affected by this change so that if you're among the 99% of our users who won't be affected you can just skip the rest of this article (parts of which are a bit technical).

Who WON'T Be Affected	Who WILL Be Affected
• On-campus users • Off-campus users who dial in to the UO • Off-campus users who simply get their IP address and other network configuration information via DHCP • Off-campus users who manually configure their system, but who have NOT manually configured their system to use the UO's name servers • Users who get an IP address in the 128.223.0.0/16 range	Users who meet **both** of the following conditions: 1. You are **not** connected via UOnet (e.g., you're connecting to the Internet using a third-party Internet service provider (ISP) such as Comcast or Qwest or Earthlink), ***and…*** 2 Even though you're **not** connected to UOnet, for some reason you **have** manually configured your system to use the UO's domain name servers (instead of using the name servers that your ISP provides for your use)

If you are one of the rare people who have manually configured your computer to use the UO's name servers from an off-campus location, name service via those UO servers will no longer work for you as of February 1. On or before that time, you'll need to reconfigure your system to use appropriate name servers instead of "bootlegging" name service from the UO's name servers.

All other users will notice no difference when this change is made.

How Do I Know If I'm Using UO DNS Servers?

To help you identify whether or not you are using one of our DNS servers, here are their names:

phloem.uoregon.edu	128.223.32.35
ruminant.uoregon.edu	128.223.60.22
dns.cs.uoregon.edu	128.223.6.9

For more information about how to verify whether or not you're using the UO's DNS servers, you can visit **http://micro.uoregon.edu/dns/**

What Is a Recursive DNS Query?

When a query is made to our DNS servers, every attempt will be made to return an IP address regardless of whether or not we are authoritative for the domain queried. This means that our DNS servers will proceed to traverse the DNS tree, recursively making queries to other DNS servers, in order to obtain an answer before responding to the client.

Why Might Someone Bootleg Name Service from the UO?

In most cases, we think that those who are bootlegging name service from the UO are doing so because their appropriate name servers—the ones that are provided for their use by their ISP—were broken or otherwise had problems. For example, on a couple of occasions in April 2005, Comcast had problems with its name servers[1]. As a stopgap measure, some Comcast users configured their systems to use other name servers (such as the UO's name servers) instead. Although Comcast's name server problems are now in the ancient past, those workarounds were never removed.

Why Must Our Name Servers Be Secured?

Disabling off-campus recursive access to the UO's name servers helps to protect the UO (and the Internet as a whole) against two types of name service-related attacks:

1. **DDoS attacks.** Name servers can be used as distributed denial of service (DDoS) attack amplifiers (the attacker sends a small spoofed UDP name service query to an open name server, forging the victim's IP address; the open name server then returns a large "answer" to the forged IP address—even though the victim didn't actually make the DNS query in the first place).

   If this is done on an ongoing basis with a large number of open name servers, it can flood the victim's IP address with responses from thousands (or tens of thousands) of name servers, thereby exhausting the victim's available network bandwidth).[2] Attacks of this sort can result in multi-Gbps flow volumes.
2. **Cache poisoning attacks.** Attackers can generate spoofed traffic to open recursive DNS servers that can result in so-called "cache poisoning" attacks,

To Be Curtailed February 1

whereby vulnerable caching name servers can be made to return bogus results for a user's name service queries.[3]

In a nutshell: The attacker "primes" the caching name server to respond to queries with an IP address of his/her choice, rather than the real/normal IP address for that site. The innocent victim asks the caching name server for the IP address of a site of interest, such as the IP address of their bank's website. If the domain name of that site happens to be one that the attacker has poisoned, the victim is automatically and transparently misdirected to a website of the attacker's choice rather than to their bank's real web page, and confidential data can then be stolen (some refer to this type of attack as "pharming")

A variant of this attack uses cache poisoning to redirect queries for popular sites (such as google.com or hotmail.com) to a site that contains a virus or other malware. If your caching name server has been poisoned, when you try to visit one of these popular sites you can unknowingly be redirected to another site that stealthily tries to infect your PC with malware.

While blocking off campus recursive access to the UO's name servers won't completely eliminate the possibility of their participating in such an attack, eliminating recursive access will substantially reduce the likelihood of their being abused.

The UO Is Not Alone When It Comes to DNS-Related Vulnerabilities

We should emphasize that the UO is not unique when it comes to DNS-related vulnerabilities. Studies have shown that as many as 75% of all the 7.5 million or so externally visible DNS servers on the Internet are open or misconfigured, providing recursive name service for arbitrary queries.[4]

The UO is committed to being a good network neighbor and to doing what we can to secure our servers and protect our local users and the Internet at large from possible UO-related DNS-based attacks. We will be taking an important step in that regard on February 1, when we secure the UO's name servers against arbitrary recursive queries as recommended by leading security authorities.[5]

Questions or Concerns?

If you're a UO faculty member, UO student, or UO staff person and have questions about the change that will occur on February 1, 2006, please feel free to contact Network Services (*nethelp@ns.uoregon.edu*) or call us at (541) 346-4395 with your concerns.

Sample Journey of an IP Address Query

Here's a sample journey of a simple query (such as 'what is the IP address of fred.example.com?') to a DNS server that supports iterative (non-recursive) queries but is not authoritative for **example.com**:

1. Resolver on a host sends query 'what is the IP address for fred.example.com?' to a locally configured DNS server.
2. DNS server looks up fred.example.com in local tables (its cache)—not found.
3. DNS replies with a referral containing the root servers.
4. Resolver sends query to a root-server for the IP of fred.example.com.
5. Root-server replies with a referral to the TLD servers for .com.
6. Resolver sends query 'what is the IP address fred.example.com' to .com TLD server.
7. TLD server replies with a referral to the name servers for example.com.
8. Resolver sends query 'what is the IP address fred.example.com' to name server for example.com.
9. Zone file defines a CNAME record, which shows fred is aliased to joe. DNS returns both the CNAME and the A record for joe.
10. Transaction complete.

Note: The above sequence is highly artificial, since the resolver on Windows and most *nix systems is a stub resolver (defined in the standards to be a minimal resolver that cannot follow referrals). If you reconfigure your local PC or workstation to point to a DNS server that only supports iterative queries, it will not work. Period.

Notes:

[1] "Another Broadband Outage Strikes Comcast" **http://news.com.com/Another+broadband+outage+strikes+Comcast/2100-1034_3-5669961.html**

[2] "The Continuing Denial of Service Threat Posed by DNS Recursion" **http://www.us-cert.gov/reading_room/DNS-recursion121605.pdf**

[3] "DNS Cache Poisoning The Next Generation" **http://www.lurhq.com/dnscache.pdf**

[4] "Domain Name Servers: Pervasive and Critical, Yet Often Overlooked" **http://dns.measurement-factory.com/surveys/sum1.html**

[5] "SANS Top 20 Vulnerabilities: The Expert Consensus"**http://www.sans.org/top20/#c6** (C6.5, "Do not allow your recursive DNS servers to be used except by your own network blocks except as required.")

The Analysis of Variance is Changing! Meet the

Robin High
Statistical Programmer and Consultant
robinh@uoregon.edu

Statistical analysis would be so simple if only a researcher didn't need to deal with all those pesky assumptions! For example, whenever you run an independent groups analysis of variance (ANOVA) you should always check three very important assumptions:

1. Observations are independent
2. Residuals computed from the group means are normally distributed
3. Residuals have equal variances across groups

The first assumption is generally met from the design, that is, by subjects randomly assigned to two or more groups.

The second assumption focuses on normality of the residuals, not the observations themselves.

The third assumption implies there is equal "spread" of the residuals, as measured by the pooled variance. Side-by-side boxplots or hilo plots for each group are particularly helpful methods for visually detecting violations in this third assumption and should always be among the initial steps of an ANOVA. Fortunately, ANOVA stands up well to minor violations of assumptions 2 and 3; however, it is not a good choice for data analysis if assumption 1 is not met.

This article introduces you to a relatively new SAS procedure called PROC MIXED, which for many applications is destined to replace PROCs TTEST and GLM. One noteworthy advantage over these two older procedures is the provisions it has for data analysis when assumptions 1 and 3 are not met. It is designed to analyze continuous or interval level response data collected across one or more classification factors which for this article will be assumed to have "fixed effects," that is, all levels of interest from each factor are included in the study.

The name MIXED implies it works with both fixed and two or more random effects, but explanation of how it works with the latter will be reserved for future articles. For now, be aware that with only a few exceptions, everything PROCs TTEST and GLM can do, PROC MIXED can do just as well—and in many situations it does it *much* better.

Mixed Model Analysis

To demonstrate how PROC MIXED works, a simple introduction is to compute a two-sample t-test from a continuous response variable collected from persons randomly chosen from a much larger population of subjects. A t-test is a special case of ANOVA with subjects randomly selected from two groups and one observation taken on each subject. Here is a "small" example dataset of test scores from an unequal number of male and female subjects selected at random:

```
PROC FORMAT;
VALUE gnd 0=' ' 1='Female' 2='Male' 3=' ';
RUN;

DATA scores;
INPUT gender score @@;
DATALINES;
1 75  1 76  1 80  1 75  1 78  1 77  1 73 1 72  1 74 1 71
2 82  2 83  2 85  2 78  2 77  2 87  2 86
;
```

The first step is to visually show the data with an informative plot. This will help determine if unequal variances across the groups exist, or if severe outliers are present. Details on how the following plotting statements are constructed can be found at
http://cc.uoregon.edu/cnews/spring2001/sasgraphics.html

```
GOPTIONS reset=all cback=white;
SYMBOL interpol=hiloj value=dot Height=1
 color=black Line=5 Width=1 Repeat=2 ;
PROC GPLOT DATA=scores;
PLOT score*gender / Noframe
       haxis=0 to 3 by 1 hminor=0
       vaxis=70 to 90 by 4 vminor=3 ;
TITLE H=2 "Test Scores";
FORMAT xplot gnd. ;
RUN; QUIT;
```

Important summary statistics from PROC TABULATE are output in table form.

```
PROC TABULATE DATA=scores NOseps ;
CLASS gender; VAR score;
TABLE gender,
 score*(n*f=3.0 min*f=4.0 max*f=4.0
 mean*f=6.2 var*f=7.3) /
 rts=12 BOX='Summary Statistics';

FORMAT gender gnd. ;
RUN;
```

```
---------------------------------------|
|Summary   |                            |
|Statistics|          score             |
|----------|----------------------------|
|          | N | Min | Max | Mean | Var   |
|----------+---+-----+-----+------+-------|
|gender    |   |     |     |      |       |
|female    | 10| 71  | 80  | 75.10| 7.656 |
|male      |  7| 77  | 87  | 82.57|14.952 |
|---------------------------------------|
```

The variances of the two levels of gender are different. But is the difference severe enough to pursue an unequal variance model? We'll check that later, but for now, because of the small sample sizes we'll assume equal variances in the two groups is probably reasonable. Rather than applying PROCs TTEST or GLM to compute a t-test of the two means under the null hypothesis of equality, the following commands from PROC MIXED produce the same results:

New Kid on the Block: PROC MIXED

```
PROC MIXED DATA=scores NoItPrint ORDER=internal;
CLASS gender;
MODEL score = gender / solution DDFM=bw;
ESTIMATE 'Female - Male' gender 1 -1 / cl;
LSMEANS gender / diff cl;
FORMAT gender gnd. ;
RUN;
```

Actually, this example demonstrates three equivalent approaches PROC MIXED offers to test two sample means for equality: by entering "solution" as an option on the MODEL statement, the ESTIMATE statement, and LSMEANS. The edited output contains this information:

```
Class Level Information

Class    Levels    Values

gender        2    Female Male
```

The residual variance of the model is found under the Covariance Parameter Estimates. Note that the standard deviation output by PROC TTEST is equal to the square root of the Estimate (e.g., 3.2518=SQRT(10.5743)).

```
Covariance Parameter Estimates
Cov Parm Estimate
Residual 10.5743
```

Since we are testing the means of a "fixed" effect, results for the t-test are observed from output produced by the MODEL statement. `'Male'` is the reference category, so Estimate=-7.4714 is the difference in the two gender means producing a t-value = -4.66 (F-value=21.74 = $(-4.66)^2$) with 15 degrees of freedom resulting in a p-value = 0.0003:

```
Solution for Fixed Effects

                             Standard
Effect   gender   Estimate   Error    t Value  Pr >|t|

gender   Female   -7.4714    1.6025   -4.66    0.0003
gender   Male      0          .        .        .

        Type 3 Tests of Fixed Effects

         Num     Den
Effect   DF      DF     F Value    Pr > F

gender    1      15      21.74     0.0003
```

The ESTIMATE statement also produces a p-value which tests the null hypothesis for equality of the gender means. How gender is coded (as printed in the Class Level Information table) defines how to place 1 and -1 on the ESTIMATE statement. By default, SAS orders levels of classification factors in alphabetical order of their formats (or in their numerical order when coded as numbers without a FORMAT or with option ORDER=internal). The two coefficients indicate to take the mean for Females and subtract the mean for Males to get the computed difference (Estimate= -7.4714). The cl option produces 95% confidence intervals for the difference of the two sample means.

```
Output from the Estimate Statement
                                     Standard
Label            Estimate     Error       DF
Female - Male     -7.4714     1.6025      15

t Value          Pr > |t|      Lower       Upper
 -4.66           0.0003      -10.8871    -4.0558
```

The same data coding features apply when working with the Least Squares Means and its associated table of differences produced by the LSMEANS statement with the option `diff`. It provides a table of the Least Squares Means (listed under the Estimate column). In this example they are the same as the actual means; however, with unbalanced data and more complicated designs this will not necessarily be the result. Their standard errors and respective confidence limits are also printed. P-values also appear on the output for LSMEANS; they usually are of little or no interest unless you want to test whether the means are different from zero.

```
Least Squares Means
                                Standard
Effect   gender  Estimate   Error      Lower    Upper

gender   Female  75.1000    1.0283     72.9082  77.2918

gender   Male    82.5714    1.2291     79.9517  85.1911
```

What is of the greatest interest is the difference between the two means. On the output for the table of differences, observe two columns labeled `gender` and `_gender`. `Female` on the line below `gender` indicates you substitute the lsmean for females, and `Male` below `_gender` indicates you substitute the lsmean for males. When you subtract them, the output shows the difference in the two means of -7.4714 (printed under the Estimate column). The standard error of the difference, the t-value, p-value, and 95% confidence limits are also printed. The t -value column is the difference between two means divided by their standard error.

```
Differences of Least Squares Means
                                                Standard
Effect   gender  _gender   Estimate     Error
gender   Female    Male    -7.4714      1.6025

DF       t Value   Pr > |t|       Lower        Upper
15       -4.66      0.0003      -10.8871     -4.0558
```

The purpose of this simple example is to show how the output from the Solution of Fixed Effects, the ESTIMATE, and the LSMEANS statements, all produce results identical to the output obtained with PROC TTEST or PROC GLM (assuming equal variances). In more complicated designs these statements have more specialized functions. The MODEL statement defines the model and produces regression-like coefficient estimates as well as tests for the fixed effects. The ESTIMATE statement allows you to estimate linear combinations of two or more group means or to probe complex interactions. The LSMEANS statement produces all pair-wise comparisons of means. Combined with the Output Delivery System, it is an extremely helpful tool when comparing differences in means.

PROC MIXED, continued…

If the variances across groups are unequal…

A statistical test for the equality of means which involves unequal variances (different from the one produced with TTEST) can also be requested with the above statements by changing the MODEL statement option for the degrees of freedom computation to DDFM=satterthwaite and adding the following after the MODEL statement:

```
REPEATED / GROUP=gender;
```

The test for equal variances involves comparing the AIC values from the Fit Statistics tables, running it with and without this REPEATED statement. How this test works and how to account for heterogeneous variances with PROC MIXED can be found at **http://www.uoregon.edu/~robinh/mixed_sas.html**. This example serves as a good starting point to understand how to embellish the PROC MIXED statements to handle a wide variety of complicated designs containing both fixed and random effects.

Mastery of these basic features gives you the background needed to graduate to more complex analyses such as repeated measurements, combinations of fixed and random effects, or hierarchical linear models, to name just a few.

PROC MIXED has been called the best thing to happen in statistical computing since sliced bread. In fact , "slice" is a helpful option for the LSMEANS statement.

Information Resources

1. Littell, R.C., Milliken, G.A., Stroup, W.W., and Wolfinger, R.D. (1996). *SAS System for Mixed Models*, SAS Institute, Cary, NC.
2. McLean, R. Sanders, and Stroup (1991). "A unified approach to mixed linear models," *The American Statistician*, 45:54-64.
3. Web articles:

   http://cc.uoregon.edu/cnews/summer2001/procmixed.html

   http://cc.uoregon.edu/cnews/summer2004/procmixed.htm

   http://www.uoregon.edu/~robinh/mixed_sas.html

The E-Shop is E-Z!

UO faculty, staff, and students can service their computer equipment right here on campus in 151 McKenzie Hall at the Computing Center Electronics Shop (E-Shop). Whether you need parts for your PC or Mac or repairs on your laptop, the E-Shop can help. Check out their services at **http://cc.uoregon.edu/e_shop.html**

The shop is open Monday through Friday from 8 A.M. to 5 P.M.

Computing Center Electronics Shop technicians perform repairs on virtually all desktop and laptop models and peripherals at competitive rates. Check in your equipment at the receiving desk in 151 McKenzie Hall. Parking is available in the McKenzie parking lot on the west side of the building.

—Minimize Your Computer's Energy Use—

Given our state's reputation as an environmental leader (and the price of electricity these days!), it is not surprising that many Oregonians want to minimize the amount of energy their computers use.

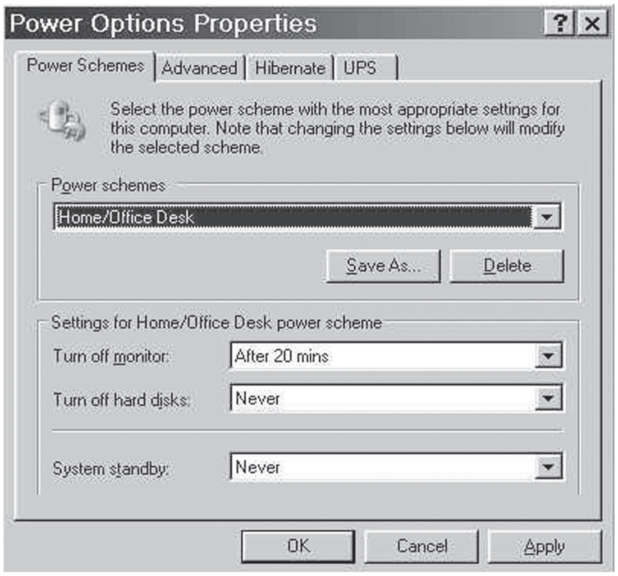
Here are some simple steps that anyone can take to conserve energy:

- If your system has the ability to "sleep" or "standby" when it's not in use, allow that function to operate
- When you purchase a new system, consider buying a laptop or an energy-efficient desktop. If you're in the market for a display, buy an LCD display rather than a traditional CRT display

Setting Your PC's Power Options

If you're running Windows XP, you can set your PC to conserve power by going to Start —> Settings —> Control Panel —> Power Options.

You'll see a panel that probably looks something like this:



Select the power scheme with the most appropriate settings for this computer. Note that changing the settings below will modify the selected scheme.

Power schemes: Home/Office Desk

Settings for Home/Office Desk power scheme

Turn off monitor: After 20 mins

Turn off hard disks: Never

System standby: Never

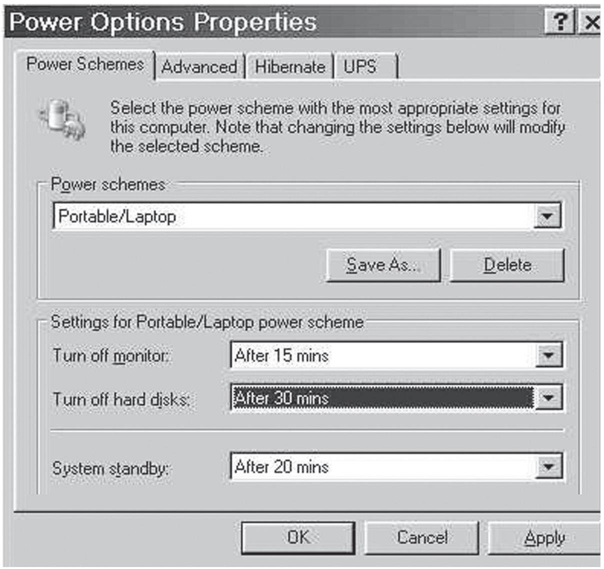
Fig. 1: Windows XP Power Options panel.

To decrease the amount of power your system uses, change the power scheme from the typical Home/Office Desktop scheme to something more aggressive. For example, you might set your desktop PC to use the "Portable/Laptop" power scheme (even though your desktop PC obviously isn't a laptop). The power scheme will then look like Fig. 2 below.

Note that the values which are shown by default aren't set in stone. For example, if you'd like to turn your hard disk off after 25 minutes or 45 minutes instead of the default 30 minutes, you can freely adjust those settings to suit your needs.

What If I'm On A Mac?

On a Mac, go to Apple Menu—>System Preferences—> Energy Saver. Adjust the sliders as desired.



Select the power scheme with the most appropriate settings for this computer. Note that changing the settings below will modify the selected scheme.

Power schemes: Portable/Laptop

Settings for Portable/Laptop power scheme

Turn off monitor: After 15 mins

Turn off hard disks: After 30 mins

System standby: After 20 mins

Fig. 2: Windows XP Power Options panel showing portable laptop power scheme.

How Much Energy Can I Save?

A typical desktop system with an LCD panel that's left on around the clock can easily consume over $100 worth of power a year. This implies that over a four- or five-year system life, the capital cost of a typical system might be matched by the cost of the power it consumes (for actual power usage cost estimates, see the power usage calculator at **http://www.eu-energystar.org/en/en_008.htm**) The simple step of enabling standby mode can easily halve that power consumption with minimum inconvenience.

An energy efficient laptop can use even less. Some energy efficient laptops may consume only $5 or $10 of power per year, although laptops often have higher initial costs (see related article regarding the emergence of budget laptops on page 28 of this issue).

Are There Times I Don't Want to Put Systems On Standby?

Sure. Some systems are inherently poor candidates for power conservation strategies. Most servers, for example, *need* to run around the clock. Similarly, if your system needs to be up at night for backup, patching, or maintenance, you wouldn't want to take power conservation steps that might interfere with those tasks.

The Savings Are Up To You

We know that when it comes right down to it, realizing energy savings at the university will be up to you. No one is going to come around and force you to make changes to how you manage your PC's power usage. We do ask, however, that you give the savings shown in this article some thought. If you can configure your PC appropriately, or make wise choices when buying a new system, the university can save a lot of money every year, and help the environment at the same time.

The Year of the $400 Budget Laptop

A closer look at rock-bottom laptop prices reveals that you can get more for your money if you're willing to pay just a little bit more up front

Joe St Sauver, Ph.D.
Director, User Services and Network Applications
joe@uoregon.edu

In the spring 2005 issue of *Computing News*, we talked a little about budget desktop systems [1], but until very recently it was hard to call any laptop "inexpensive." The post-Thanksgiving "Black Friday" sales of 2005 changed all that. A variety of retailers made history by offering laptops for around $400 after rebates and special discounts. That's an amazing price, and one which drew the attention of many consumers, including users here at the University of Oregon.

Two questions that many users asked were "How *did* they get the price of those laptops so low?" and "Would one of those systems work well for me?"

Arriving at a Targeted Price Point

Looking more closely at the laptops with rock-bottom prices, you'll notice that an extremely "sharp pencil" has usually been applied to their configuration. Economies have often been realized through:

- **Use of a lesser LCD display** (budget laptops may use smaller and/or less vibrant displays than higher-end laptops)
- **Use of a Celeron or Sempron CPU rather than a more powerful processor** (however, if you're just browsing the web or using a word processor, you may never notice the difference)
- **Use of Windows XP Home rather than XP Pro**
- **Reduction in the amount of main memory, down to 256MB from a more typically recommended 512MB** (and 64MB or more of that 256MB may be reserved for use by the integrated video adapter, leaving just 192MB or less for use by your applications)
- **Use of smaller hard drives** (e.g., where many laptops are routinely seen with a 60GB hard drive now, a budget laptop may have only a 40GB hard drive)
- **Use of a smaller capacity or shorter run-time battery** (battery run times may be down in the one-hour range for some budget systems)
- **Omission of WiFi wireless network connectivity**
- **Substitution of a CD read-only drive (or a CD/DVD read-only drive)**, instead of including a CD read/write or CD/DVD read/write drive
- **Little (if anything) in the way of bundled software**
- **No CD copy of the operating system**
- **Limited printed documentation**
- **Minimal warranty duration and warranty terms**
- **Shipping and handling charges.** In the case of laptops purchased online, shipping and handling charges may run 10% to 15% of the cost of the laptop itself

Can You Live With That?

When you consider that stripped-down configuration, some of those economies may matter to you and others may not. It really depends on the demands of your applications and your expectations.

For example, consider the issue of the limited battery capacity of budget laptops: if you use your laptop primarily in locations where you can easily get access to wall power, such as in a motel, limited battery capacity may only be a minor consideration. On the other hand, if you frequently fly coast-to-coast, a one-hour battery would dramatically limit your ability to work while airborne during those longer flights.

Of course you could always buy a spare higher capacity battery, but be aware that it is not uncommon for a spare laptop battery to run $100 or more—fully a quarter of your budget laptop system's nominal cost.

Another example of an economizing measure that may or may not matter greatly to you is memory capacity: you may run very simple applications, or you may be able to tolerate relatively slow performance, or you may be able to upgrade your laptop from 256MB of memory to 512MB or more, but be sure to figure the cost of that upgrade into the total cost of the system (including any installation charges, if you're not comfortable doing that work yourself).

As a final example, consider a laptop that comes without integrated wireless. You could add an external wireless card, but that may not be as convenient as having an integrated wireless setup—and again, this would raise the final cost of the system.

Aggressive Salesmanship

When purchasing a budget laptop you should also be aware that at least some retailers may train sales staff to do an aggressive job of pushing add-ons such as:

- **System "tune-ups"** ("We can remove a lot of the default applications that ship with your system and gobble up precious memory. Once we do that, your system will run substantially faster. Our nominal fee for that is just...")

- **Extended warranties** ("While your new laptop comes with a 90-day warranty, we can fix you up with a two-year extended warranty that will give you peace of mind for only another ...")
- **Software** ("Your new laptop doesn't come with a word processor or any antivirus software. Would you like to buy Office and a security suite?"

  [Remember that OpenOffice (free) is an option for basic word processing [2], and that the UO site-licenses McAfee, a commercial antivirus/antispyware product, for use by faculty, students and staff.]
- **System accessories/upgrades** ("Don't you want a nice case to protect your new system? How about an external floppy disk drive? While you're here we can double your memory for the low, low price of just ...")

If it's important for you to keep the cost of your system low, a key phrase to remember is, "No thanks, I just want the laptop."

Combination Offers

In other cases, in order to qualify for an amazing price on a laptop you might need to sign up for hundreds of dollars worth of service through a third party ISP, or apply for a credit card (which may have annual fees or other associated costs).

Missed Rebates

Many retailers are also counting on at least some fraction of purchasers failing to correctly complete and submit their rebate requests in time. Don't let this happen to you! Double-check the requirements needed to receive your rebate, and be sure to keep a copy of all the materials you submit.

By the time you've added up all these factors, it becomes evident that a super-cheap laptop may ultimately not be much of a bargain.

What If You're Willing to Pay a Little Bit More?

If your budget allows you to raise your price point just a little, you may be able to get a lot more for your money. This December we saw multiple laptops from name-brand manufacturers such as Compaq, Dell and Toshiba in the $500-$550 price range (after rebate) that had all or most of the features you'd likely want, including:

- full-sized bright and crisp displays
- 512MB of memory
- 60 gig hard drives
- integrated wireless
- one-year warranties… and so on

At least in some cases, those $500-$550 systems were bundled with a free (after rebate) printer [3] and a free (after rebate) wireless access point. [4]

At that price, those systems may very well be worth your consideration. When all is said and done, those $500-$550 laptops may be the real bargains of the 2005 holiday season, not the much-ballyhooed (but far less capable) $400 laptops.

What About Used Laptops?

Sometimes users wonder if there are bargains to be had in the used laptop market; in general, we'd urge you to be cautious about buying used laptops for a few reasons:

1. **Laptops are a top target of thieves.** You may accidentally buy a "used" laptop that's actually been stolen. Make sure you know your seller and the provenance of the system you're considering.
2. **Laptops can get hard use and become damaged, sometimes in inconspicuous ways or ways that only show up on an intermittent basis.** It can be easy to buy a used laptop that's a lemon.
3. **Even if a laptop hasn't been damaged or abused, normal wear and tear can add up.** For example, normal charge and discharge cycles can reduce the ability of a laptop's battery to hold a charge (and as mentioned previously, replacement batteries aren't cheap).

4 **A laptop that's even a year or two old will often be significantly less powerful than current systems.**

5 **Used laptops may come completely "bare."** This may not be a problem if you plan to run Linux on your laptop, but if you plan to run Windows, you'll want to make sure your used laptop at least comes with a valid license for Windows XP.

7. **Ironically, used laptops can often cost more than new promotionally priced laptops.**

How Do You Find Bargain Laptop Deals?

Curiously enough, some of the best bargain laptop deals are often advertised in advertising inserts in the local Sunday *Register Guard*. If you check the paper and find a system that looks like a real bargain, be sure to go to the retailer early in the day because some particularly good bargains sell out fast, and rain checks will usually not be available.

Another good source for bargain laptop deals is the "Hot Offers" or "Online Deals" section of major laptop vendor websites (Dell tends to have particularly deep online discounts from time to time, but note that Dell's offers can vary dramatically on a *daily* basis).

- continued on page 30

$400 Laptops, continued…

Other users swear by online websites that specialize in collecting online vendor coupon codes and special manufacturer promotional deals (see the listings at **http://www.uoregon.edu/~joe/deals.html**)

A caveat: We recommend that you do *not* "register" or give your email address to *any* deal or promotional site. Visit deal sites on the web, sure. Check them out via RSS if you like, absolutely. But we recommend that you do *not* sign up for emailed deal notices or new product bulletins. Most such sites are very good about respecting your privacy, but some may share your email address with marketing partners and you may be inundated with spam as a result.

One Last Thought about Deal Sites

Deal sites, like online auction sites, have a uniquely engrossing quality. It is easy to lose site of the objective and spend a tremendous amount of time and effort just looking for ever better deals. Don't let a casual search for a good deal turn into a life-disrupting obsession.

Notes:

[1] "Budget Desktop Systems: Are They Right for You?" **http://cc.uoregon.edu/cnews/spring2005/budget.htm**

[2] **http://www.openoffice.org** (also see Spencer Smith's review of OpenOffice on pp. 14-15 of this issue)

[3] Be aware that required cables are often not included and will cost extra, and that the cost of a printer may be negligible in the long term relative to the cost of consumable supplies (such as ink cartridges for your printer). The strategy of giving away printers reminds me of the comment attributed to a film company executive: "Give away cameras; we'll make our money on the film."

[4] If you get a personal wireless access point, please use it only at home. On campus, deployment of personal wireless access points can interfere with the official campus wireless network or introduce security vulnerabilities that impact the campus as a whole. If you need information about wireless network access on campus, please see **http://micro.uoregon.edu/wireless/**

More About Laptops

MIT's $100 Laptop Project

While we're talking about budget laptops, it is impossible to avoid mentioning MIT's highly publicized $100 Laptop Project, aimed at making $100 laptops available to children in the developing world (see **http://laptop.media.mit.edu/**).

Please note (as mentioned on the MIT $100 Laptop site) that these $100 laptops are not yet in production. Once they are, they will only be distributed directly to schools through large government initiatives, and you will not be able to buy one directly.

What About Sites That Offer "Free" Laptops?

If you Google for "free laptops" you'll typically see a variety of web pages that offer "free" laptops.

Just as there is no free lunch, there is no such thing as a truly free laptop—at least not one that doesn't have lots of strings attached. Read the fine print at those sites, and you'll see that receipt of your "free" laptop will typically require you:

- to divulge personal information
- to accept a deluge of marketing offers from the company and its affiliates
- to comply with requirements that may be expensive or virtually impossible to perform ("Oh, I'm so sorry. I'm afraid you didn't complete all the terms of the offer, and so you're not eligible for your free gift after all")

Don't get suckered! As noted on **http://www.lookstoogoodtobetrue.com/** (a website developed and maintained by a joint federal law enforcement and industry task force): If an offer looks too good to be true, it probably is!

free tech training: workshops on demand

The UO Libraries offers *Workshops on Demand*, a new model of technology training to faculty, staff, and students that emphasizes increased collaboration with faculty in integrating information technology skills into the curriculum. See **http://libweb.uoregon.edu/it/** for full details.

Spotlight on Security

Two New Highly Critical Vulnerabilities Affect IE, Symantec Antivirus Products

Two highly critical new vulnerabilities emerged at the end of December:

1. **IE 5.5 and 6.x.** Secunia is reporting a vulnerability in Internet Explorer 5.5 and 6.x that allows arbitrary code to be executed on a vulnerable browser if the user is tricked into visiting a malicious website (as may occur when clicking a malicious link masquerading as an e-card link, for example). For details, see **http://secunia.com/advisories/15546/**

Users are advised to use Firefox instead of IE; if you must use IE, be sure to keep your patches up-to-date.

2. **Symantec Antivirus products.** FrSIRT has released a critical vulnerability warning for Symantec Antivirus products relating to how certain malformed RAR files are handled. This vulnerability could allow attackers unauthorized control of data and related privileges and could even cause further network compromise. Symantec users are likely vulnerable regardless of whether they choose to open or read an infected email.

SANS is now reporting that Symantec has released updated definitions that block the malformed RARs that are at the core of this exploit:

http://isc.sans.org/diary.php?storyid=949

http://www.symantec.com/avcenter/venc/data/bloodhound.exploit.55.html

If you are still running Symantec Antivirus products, immediately update your antivirus definitions or migrate to McAfee. For details on the vulnerability, see

http://secunia.com/advisories/18131/

http://www.frsirt.com/english/advisories/2005/3003

Extremely Critical .wmf File Vulnerability

At the end of December an extremely critical vulnerability was discovered in the handling of Window Metafiles (.wmf files). It can be exploited to execute arbitrary code, and exploits are triggered automatically when an ususpecting user visits a malicious website using Internet Explorer (see **http://secunia.com/advisories/18255/).** You may download the patch from **http://www.microsoft.com/downloads/details.aspx?FamilyID=0c1b4c96-57ae-499e-b89b-215b7bb4d8e9&DisplayLang=en**

December's Microsoft Patch Fixes Earlier 'Critical' Internet Explorer Flaw

This IE vulnerability is yet another flaw that could allow an attacker to take control of an affected system. For details, see Microsoft's December 2005 Security Bulletin Summary at **http://www.microsoft.com/technet/security/bulletin/ms05-dec.mspx** Or, if you just want to make sure you get patched, run Microsoft Update (or Windows Update) from the Start menu or visit Microsoft Update at **http://update.microsoft.com/microsoftupdate/**

Note to UO Windows users who use Blackboard with IE: *Because of the high number of security vulnerabilities that recur in Internet Explorer, we recommend you switch to the latest Firefox web browser if at all possible.* If you continue to use IE with Blackboard, be aware that it requires JavaScript active scripting. If you disable active scripting in IE as a security measure, or set the IE browser security preference to "high," Blackboard won't work. To ensure that your browser is configured properly, go to **http://libweb.uoregon.edu/cet/blackboard/plugin/#browser**

Phishing Exploit Poses as UO Security Email

The first week of December, Network Services security engineers reported seeing a phishing attempt to send emails from "security.uoregon.edu". These bogus emails asked users to "confirm their email" or have their accounts suspended. Fortunately the phishers did no harm, as the messages were delivered in the middle of the night and the clickable link they contained was dead by 6 A.M.

Please remember to be suspicious of links that come in email or instant messaging. The best security practice is to not click on *any* link that comes to you via email, even if it appears to be from a person or organization that you know. Phishing ploys have become so sophisticated that it is virtually impossible to tell a counterfeit site from a real one.

Sober Worm Disrupts Email

On December 2 email traffic slowed virtually to a halt between Comcast account holders and users of Microsoft-based Hotmail, thanks to a variant of the Sober worm. The Sober worm first appeared in 2003 and infects Windows PCs, causing the infected machines to repeatedly send spam emails that negatively impact network performance. For details, see the Sober-Y article on page 16 of this issue, and *ZDnet's* report at **http://news.zdnet.co.uk/internet/security/0,39020375,39240173,00.htm**

More Than Two Million Domain Names Registered with False Data

The U.S. Government Accountability Office (GAO) recently reported that millions of Internet domain names have been registered with false or incomplete information, possibly in an attempt to hide the owners' identities or to prevent the public from contacting them. For details, see **http://www.networkworld.com/cgi-bin/mailto/x.cgi?pagetosend=/export/home/httpd/htdocs/news/2005/120905-domain-names.html**

Flaw in All Versions of Veritas NetBackup

Last October, a serious security hole was discovered in all versions of NetBackup that could allow attackers to execute arbitrary code with root/SYSTEM privileges. You'll find more details on this vulnerability, including a maintenance pack to fix it, at **http://seer.support.veritas.com/docs/281107.htm**

COMPUTING CENTER GUIDE

UO Website
http://www.uoregon.edu/

Computing Center Website
http://cc.uoregon.edu/

Microcomputer Services
(151 McKenzie Hall)
http://micro.uoregon.edu/
346-4412
microhelp@lists.uoregon.edu

- microcomputer technical support
- help with computing accounts, passwords
- scanning, CD burning, digital video
- help with damaged disks, files
- system software help
- Internet connections, file transfers
- public domain software, virus protection
- software repair (carry-in only, $80/hour, 1/2 hour minimum)

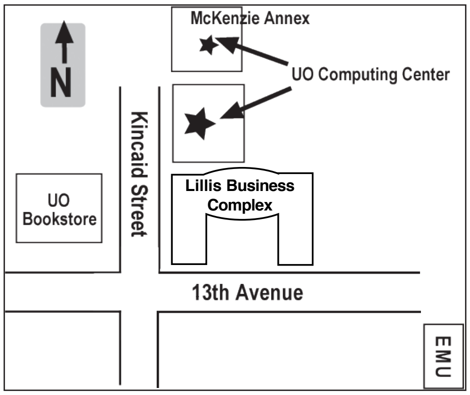
Documents Room Library
http://docsrm.uoregon.edu/
(175 McKenzie Hall)
346-4406

Modem Number
Dialin modem number for UOnet, the campus network: **225-2200**

Large Systems Consulting
http://cc.uoregon.edu/unixvmsconsulting.html
(225-239 Computing Center)
346-1758
consult@uoregon.edu

- Unix
- email, multimedia delivery
- scientific and cgi programming
- web page development

Statistics Consulting
Robin High
219 Computing Center
346-1718
robinh@uoregon.edu



Electronics Shop (151 McKenzie Hall)
http://cc.uoregon.edu/e_shop.html
346-3548
hardwarehelp@uoregon.edu
Computer hardware repair, upgrades

Network Services
http://ns.uoregon.edu/
346-4395
nethelp@ns.uoregon.edu
Central data communication and network services

Telecommunications Services
http://telcom.uoregon.edu/
346-3198
Local and long distance phone service for the UO campus.

Administrative Services
http://ccadmin.uoregon.edu/
346-1725
Programming support for campus administrative computing.

Computing Center Hours

Mon - Fri	7:30 A.M. - 5:00 P.M.

McKenzie Building Hours

Mon - Thu	7:30 A.M. - 11:30 P.M.
Friday	7:30 A.M. - 7:30 P.M.
Saturday	9 A.M. - 9:30 P.M.
Sunday	9 A.M. - 9:30 P.M.

- Note: These are *building* access hours; hours for individual facilities may vary.

O
UNIVERSITY OF OREGON
UO COMPUTING CENTER
1212 University of Oregon Eugene, OR 97403-1212