University of Oregon

COMPUTING NEWS

Summer 2003

A sculpture by Northwest artist Lee Kelly reflects the summer light on the Straub Hall Quadrangle.

IN THIS ISSUE...

Campus Wireless Coverage Expanded

New coverage gives wireless users more options

Dale Smith
Director, Network Services
dsmith@ns.uoregon.edu

Over the past several months, the Network Services group has expanded wireless coverage to include a number of new areas on campus. Thanks to their efforts, you'll now be able to use your laptop in the following additional locations:

- Gilbert (East and West)
- Chapman (second and third floors)
- Straub first floor (includes most public areas and classrooms around Room 146)
- Gerlinger (second and third floor classrooms and Gerlinger Lounge)
- Education and Education Addition buildings
- North Site (including Fine Arts buildings and all the Millrace buildings)
- Student Rec Center (public area and lounge around the juice bar)
- Additional coverage areas in the Knight Library.

For more details, including a map of campus wireless coverage, see **http://micro.uoregon.edu/wireless/**

Got Any Suggestions?

We would like to solicit suggestions for additional coverage areas for future wireless projects. Top consideration will be given to areas used by students for study and/or research activities.

If you have ideas for future wireless expansion, contact Network Services Director Dale Smith (**346-1745**, *dsmith@ns.uoregon.edu*).

UNIVERSITY OF OREGON

COMPUTING CENTER

COMPUTING NEWS
VOL. 18 #3

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

Contact: Joyce Winslow
jwins@oregon.uoregon.edu

Photography: Dave Ragsdale
dave@oregon.uoregon.edu

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

Need a Laptop? Consider the UO Libraries' New Laptop Loan Program

Ron Renchler
Director, Library Communications
ronr@darkwing.uoregon.edu

If you're a student who needs a laptop so you can do your academic work anytime, anywhere, the UO Libraries can help.

Nine new laptop computers—seven Dell Latitude D600 (Windows) and two Macintosh iBooks—are available to students for checkout in four-hour blocks during weekdays. The laptops also may be checked out overnight or for a full weekend. The UO Libraries' Media Services Department, located in Knight Library, is handling the checkout process.

To borrow a laptop, you must have a current UO student ID and a second piece of identification with your picture and signature on it.

Microsoft Word, Excel, PowerPoint, and Internet Explorer, along with other basic software, are preloaded on the machines, which also offer network connectivity and printing capabilities. The laptops are configured to work with other equipment, such as digital cameras, that students may check out from Media Services.

For complete information about the laptop loan program, see **http://libweb.uoregon.edu/med_svc/laptops/**

This site contains links to an online advance reservation system and information on loan periods, fines and liabilities, theft prevention, and networking the laptops. *(Overdue fees and charges for damage or loss are substantial, so please read the checkout information carefully before using this service.)*

The laptop loan program is offered through the UO Libraries with funding from the 2002-2003 Education Technology Fee program. Contact Media Services (**346-3091**, *mediasvc@oregon.uoregon.edu*) for more information.

A Quick Summer Refresher Course on Keeping Your Computer Secure

Three simple precautions can save you grief in the long run

Jon Miyake
Acceptable Use Policy Officer
miyake@uoregon.edu

This is the time of the year that new computers are purchased and old ones are passed on down the line.

No matter how you came to have that new (to you) computer on your desk, you will want to do some or all of the following simple things to help keep your computer secure:

1. Install Norton AntiVirus

Symantec Norton AntiVirus (NAV) is site-licensed to the University of Oregon for use by faculty, staff, and students on their campus and home computers.

You can download Norton AntiVirus from the Duckware CD-ROM, which is updated and distributed on campus each fall. In addition, NAV is always available from the public domain server at **http://public.uoregon.edu/**

For more details about antivirus protection, contact Microcomputer Services at **346-4412** or visit their antivirus information page (**http://micro.uoregon.edu/av/**).

After installing NAV, you will want to update its definitions and scan your computer for viruses. We recommend that you keep auto-protect turned on, enable automatic update ("LiveUpdate") of virus definitions, and schedule NAV to scan your computer at least once a week, if not more often.

2. Check for and Install Updates and Patches

It is equally important to keep your system current by installing security-related system updates and patches.

We recommend that most users make use of whatever automatic updating features their operating system supports. Although auto-updates are a controversial issue in the tech community, they will nonetheless provide you with the greatest amount of protection from remote exploits with a minimal amount of effort.

3. Disable or Remove Services That Are Not Being Actively Used

If you are not actively using a service, (e.g., HTTP, FTP, SMTP), turn it off. Many of the computer break-ins we see on campus are related to a seldom-used service being remotely compromised.

Disabling a service may require the assistance of someone with an advanced understanding of your particular operating system. Please refer to your local technical support person for assistance (a list of support staff is available at **http://deptcomp.uoregon.edu/local/index.html**).

Beyond the Basics

The three security steps outlined above are some of the simple things that can be easily done by users with moderate computer skills. It is obviously not an exhaustive list.

Individuals who are dealing with sensitive information or maintaining departmental servers will want to take additional steps to further secure their systems from attack.

Contact Network Security (*security@uoregon.edu*) to learn some additional steps you can take to protect your computer.

What Happens to Your UO Email Account Over the Summer?

Can you still use your UO account when you take a term off, or graduate?

If you're planning to take the summer off and return to studies this fall, will you still be able to access your UO email account?

The answer is yes! All students who take a term off and then register for classes the following term can continue to use their computing accounts without interruption.

However, if you take more than one consecutive term off before reregistering, expect that your account will be disabled. (Your account gets disabled during the second term in which you've failed to reregister.) This policy also applies to students who are on leave or who are involved in a program that causes them to not show current term credits for more than one term.

What if you graduate? After you graduate, you will normally get one free "vacation term" before your account is deactivated. In addition, the UO Alumni Association now offers a free email alternative. See **http://alumni.uoregon.edu/** for more information.

If you have further questions about your UO email account, call Microcomputer Services at **346-4412** or visit the Help Desk in 151 McKenzie Hall weekdays from 9 A.M. to 5 P.M.

Reminder: Intercampus Telephone Calling Now Requires 12-digit Dialing

Dave Barta
Manager, Telecom Services
dbarta@uoregon.edu

Since the new OUS Telecom System 12-digit dial plan went into effect on July 1, UO phone system users have no longer been able to call other OUS Institutions by dialing only five digits.

To call someone at PSU, for example, you now must dial 9-1-503-725-xxxx instead of 5-xxxx. However, campus users can still use the five-digit plan to call within the UO campus and can still place calls to other OUS institutions without entering long distance authorization codes.

Why the Change?

This change is the result of increased use of telephone numbers throughout OUS. In 1989 we acquired numbers for all the campuses comprising a unified numbering plan with no duplicate five-digit extensions across the system.

But after 14 years, growth has caused some schools to expand beyond their original number allocations, causing duplicate five-digit extensions within the system and signalling the end of the OUS-wide five-digit plan. This is similar to the changes that forced the entire Portland local calling area to move to ten-digit dialing for all calls.

Other impacts of the change:

This 12-digit dialing change can affect more than just the way you place long distance calls to other OUS institutions.

Speed dialing lists will be reprogrammed by Telecom Services, but you may have to reprogram certain features (such as auto dial buttons and voice mail out-calling) yourself. Sending and receiving Audix voicemail messages from other campuses has also changed.

Audix Addressing

Addressing messages to AUDIX subscribers *within* an institution will still use five digits and will provide name confirmation of the addressee.

Addressing messages to and receiving message from AUDIX subscribers at *different* institutions will have the following requirements and functions:

- 11 digits are required when addressing.
- The first digit of the 11-digit number corresponds to the AUDIX system of the person to whom the message is addressed (e.g. 1, 2, 3). OHSU, OSU, and UO have more than one system. To determine the first digit (1, 2, 3, etc.) for OHSU, OSU and UO, go to **http://inoc.ous.orst.edu/dialplan/**
- The last 10 digits of the 11-digit number correspond to the telephone number (area code and number) of the person to whom the message is addressed.
- An access code of nine (9) is not required when addressing Audix messages.
- Message reply to a subscriber at a different institution is provided.

Resources

You'll find programming assistance, answers to frequently asked questions, and dialing instructions online at
http://telcom.uoregon.edu/12-digit-dialing.htm

A number-finding tool is also available at **http://inoc.ous.orst.edu/dialplan** We recommend bookmarking this website, as well as saving the conversion table on the opposite page for future reference.

OS X TIP:

ADDING TO THE DEFAULT MENU

OS X is a great operating system, but there are a couple of things it fails to include in its default menu "out of the box." Below we've described how to add three useful actions to the menu bar:

- **Locking the Screen From The Menu Bar**
  1. Use the Finder to go to the Applications Folder --> Utilities --> Keychain Access --> View
  2. Make sure "Show Status in Menu Bar" is checked (you should see a padlock icon appear in the menu bar)
- **Ejecting a CD From the Menu Bar…and more**
  1. Use the Finder to go to System —> Library —> CoreServices —>Menu Extras
  2. Drag Eject.menu to your menu bar.
  3. While you're there, you'll see some other items you may also want to drag to the menu bar, including **Clock.menu, Volume.menu, and Displays.menu**

OUS Extension-to-Phone Number Conversion Table

(Sorted by Extension Number)

5-digit extension	11-digit phone number	Campus
1-4000 to 1-4999	1-503-751**-4000** to 4999	WOU
1-5000 to 1-5999	1-541-851**-5000** to 5999	OIT
1-6000 to 1-6999	1-541-201**-6000** to 6999	SOU
1-7000 to 1-8999	1-503-471**-7000** to 8999	PSU
2-3000 to 2-4499	1-541-962**-3000** to 4499	EOU
2-6000 to 2-8999	1-541-552**-6000** to 8999	SOU
3-0000 to 3-9999	1-541-713**-0000** to 9999	OSU
4-0000 to 4-9999	1-503-494**-0000** to 9999	OHSU
5-0000 to 5-1999	1-541-885**-0000** to 1999	OIT
5-2000 to 5-9999	1-503-725**-2000** to 9999	PSU
6-0000 to 6-9999	1-541-346**-0000** to 9999	UO
7-0000 to 7-0099	1-541-737**-0000** to 0099	OSU
7-0100 to 7-0399	1-541-867**-0100** to 0449	OSU- HMSC
7-0450 to 7-0874	1-541-737**-0450** to 0874	OSU
7-0875 to 7-0899	1-541-867**-0875** to 0899	OSU - HMSC
7-0900 to 7-9999	1-541-737**-0900** to 9999	OSU
8-0000 to 8-7999	1-503-418**-0000** to 7999	OHSU
8-8000 to 8-9799	1-503-838**-8000** to 9799	WOU

iRider: Cool New Web Browser for Windows

Joe St Sauver
joe@oregon.uoregon.edu

If you try only one new piece of software this year, make it the new iRider web browser. You can download a free trial version from **http://www.irider.com/** (if you want to keep using it after the three-week trial period, you need to buy it for $29). Or, check out the Flash demo at **http://www.irider.com/demo/demo.htm**

Feedback: If you try iRider, I'd be interested to know what you think. Drop me a line at *joe@oregon.uoregon.edu*

Looking for a Spyware Removal Tool? *Spybot Search & Destroy* Gets the Job Done

Patrick Chinn
Distributed Network Computing Consultant

pchinn@uoregon.edu

A new contender is challenging LavaSoft's AdAware as the top spyware removal tool.

It's called Spybot, and PepiMK Software launched version 1.0 in June 2002 (the current version of Spybot is 1.2).

Spybot Search & Destroy is available for free, although the author will graciously accept donations to support the product's development. If you want to download Spybot, visit **http://security.kolla.de**

What's Spyware? Spyware is any software that employs a user's Internet connection in the background without the user's knowledge or explicit consent.

Often spyware is used by companies to track an individual's web surfing habits and send that data back to a central database. Spyware is not necessarily illegal, but privacy concerns with how that marketing data is used has resulted in spyware detection and removal tools like AdAware and Spybot Search & Destroy.

How Spybot works. Like AdAware, Spybot scans your Windows PC for spyware components and presents a list of its discoveries. The user then has the option to remove some, all, or none of the items found.

Spybot also has an update feature for spyware profiles and help files. The feature is not automatic, like Symantec's LiveUpdate. Instead, the user must click the "Search for Updates" button and then select which updates to download and install. An automatic update feature would be more convenient, but this design still provides some convenience to adding new spyware profiles to Spybot.

Unique to Spybot is its Opt Out feature, found in the Online section. Opt Out contains a list of the most common email advertising lists. If you have opted in to an advertising list in the past and no longer remember how to opt out, double-click on the appropriate entry in Spybot to create an opt-out email message or to visit the opt-out web page on the company's website. *(Note: As a general rule, the Computing Center does not recommend that you attempt to unsubscribe.)*

Tech support. Technical support for Spybot Search & Destroy is limited to built-in help and PepiMK Software's website. No telephone technical support is available. (This is not unusual for a free product written by one person.) The built-in help is reasonably thorough, and the website offers more information and discussion forums about the product.

Spybot Search & Destroy is available for Windows only. Although Macintosh and Linux computers can also be affected by spyware, most of the insidious spyware components run under Windows only.

Spammers Target Hotmail… Big Time

Joyce Winslow
jwins@oregon.uoregon.edu

A new Microsoft vulnerability that's being exploited by spammers has been causing major email headaches since March.

Holes in Hotmail's WebDAV interface have allowed spammers to script automatic spam runs, contributing to a huge increase in spam—all with forged sender addresses. Microsoft has taken some steps to correct the problem, but Hotmail remains vulnerable as we go to press.

For more details on the Hotmail debacle, see Chip Rosenthal's commentary ("Hotmail Vulnerability Being Exploited by Spammers") at

http://www.unicom.com/chrome/a/000262.html

At the University of Oregon, we've taken steps to protect our users from this latest spam blight by blocking some (but not all) email from MSN/Hotmail.*

**** Late-breaking news:***

Microsoft appears to have been able to ameliorate this problem, so we've lifted this block. However, there is some debate over Microsoft's dedication to resolving the spam issue See "Microsoft anti-spam campaign 'hypocritical'" at

http://news.zdnet.co.uk/story/0,,t278-s2136652,00.html

Mathematica Site License Renewed

The UO's site license for Mathematica software has been renewed for another three years. License codes have been distributed to the appropriate departmental contacts, and you can request updated license codes from them. Mathematica contacts are listed at **http://darkwing.uoregon.edu/~hak/mathematica_reps.html**

Who's Sending Email? Ask IronPort

A behind-the-scenes look at email traffic: some of the top senders may surprise you

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

Have you ever wondered who are the biggest senders of email on the Internet? IronPort Systems can help answer that question on their website at **http://senderbase.com/**

We looked at IronPort's site on May 27th. Some of the top senders for the 24 hours preceding that date are domains that would hardly surprise anyone: **yahoo.com** is in first place with approximately 679 million messages per day, with **Hotmail** next at approximately 375 million messages per day.

Other well known top-sender domains included **attbi.com** (349.2 million), **rr.com** (305 million), **aol.com** (252 million), and **comcast.net** (233.7 million).

But some of the other top senders are more surprising:

• **online-shop-exchange.com**, part of VMX Inc., has an estimated daily volume of 314.1 million. Add to that the 288.6 million associated with **shoppersville.net**, also part of VMX Inc., and the total, an estimated 602.7 million messages per day, would put this particular sender second only to yahoo.com in terms of total message volume.

To put these numbers in context, if you wanted to deliver 600 million messages per day, you would be required to deliver over 6900 messages per second, around the clock. That's a lot of email!

• **ew01.com**, which is part of WholesaleBandwidth, Inc., sent an estimated 94.6 million messages during a 24-hour period on May 26.

• **dartmail.net**, part of Doubleclick, Inc., sent an estimated 92.8 million messages in one 24-hour period.

The InPort Systems website also lists the top senders by IP address.

All in all, this is a fascinating site if you're trying to understand what's being sent in terms of email traffic volumes.

« sites worth seeing »

1. **Webby Awards winners for 2003…**To see all the Webby nominees and winners for the top websites of 2003, go to:
   http://www.webbyawards.com/main/webby_awards/nominees.html
2. **National Do Not Call Registry…** Call **1-888-382-12222** or register online to block telemarketers from calling or emailing you. (You might also want to check out Oregon's do-not-call list plan at **https://www.ornocall.com/**).
   http://donotcall.gov/
3. "**Certificate Management and Installation with OpenSSL**"**…** Guidelines for advanced applications of OpenSSL. Extensive, detailed coverage of how to work with a variety of certificates, including those for mobile devices, as well as configuring pine and mutt to use TLS/SSL
   http://tirian.magd.ox.ac.uk/~nick/openssl-certs/
4. "**From PlayStation to Supercomputer for $50,000**"**…** *New York Times* article (John Markoff, May 26) on the astounding computing power of some video-game consoles, as demonstrated by the National Center for Supercomputing Applications at the University of Ilinois at Urbana. Using "an army" of Sony PlayStation 2's, university researchers assembled a supercomputer capable of an estimated half-trillion operations a second.
   http://www.nytimes.com/2003/05/26/technology/26XSUPE.html?th
5. **"Denial of Service via Algorithmic Complexity Attacks"…** Paper by Rice University's Scott A. Crosby and Dan S. Wallach demonstrating how a new class of low-bandwidth denial of service attacks can exploit common algorithmic deficiencies in many data structures.
   http://www.cs.rice.edu/~scrosby/hash/CrosbyWallach_UsenixSec2003/
6. **UO VPN Software for OS X…** The UO has VPN service available for off-campus broadband users that encrypts traffic from your system to campus. VPN service also assigns you a UO IP address, which means you will be able to access a number of resources restricted to UO users only. To get set up to use the VPN service with OS X, see the VPN link in the Mac OS X "Off Campus" section at
   http://micro.uoregon.edu/getconnected/index.html
7. **NSF Strategic Plan Available Online…** If you're planning to seek National Science Foundation support for your research, you may want to see NSF's current strategic vision, goals, priorities, and procedures at
   http://www.nsf.gov/od/stratplan_03-08/draft-stratplan.htm

Videoconferencing Quietly Thriving

Improved quality, convenience, and cost savings contribute to the increasing popularity of videoconferencing technology

Craig Leavy
Videoconferencing Engineer, Telecommunications Services
cleavy@uoregon.edu

Videoconferencing is alive, well, and quietly thriving throughout the University of Oregon campus. From job candidate interviews to defense of doctoral theses, from project management to distance education, videoconferencing is providing the answer for both students and staff looking to connect with colleagues around the world.

The main reason videoconferencing has become such a popular medium for many types of collaborative meetings is that it saves time and money. Videoconferencing's high quality and ease of use is encouraging a growing number of people in the campus community to use it, rather than traveling long distances to meetings and seminars.

A Videoconferencing Primer

Videoconferencing is a way to see and talk with others in real time via an interactive audiovisual meeting channel. The ability to display full-motion video and to hear contiguous, full-duplex audio conversations (meaning both parties can speak simultaneously, as is possible via the telephone) is accomplished by sending compressed audio and video signals over long-distance telephone networks or the Internet.

Videoconferencing systems employ codecs, which compress audio and video signals into digital data, and then decompress them at the far end, or "receive" sites. By connecting sites around the world, either in a point-to-point configuration, or in a bridge call (connecting three or more parties), participants on both the near and far ends are able to see and speak with each other while their respective images are displayed on conventional television monitors or projected onto larger screens.

To ensure that videoconferencing systems from different manufacturers can work together seamlessly, the industry has established a suite of common operating standards. These standards set the parameters for the important criteria of each call, such as the speed of the connection (measured in bandwidth), audio quality, camera control and alignment, and various other signaling information.

The suite of standards used for ISDN telephone line-based systems is known as H.320. The suite of standards for Internet Protocol (IP)-based systems is H.323.

H.320 systems are more widely in use today, but the newer H.323 systems are now saturating the marketplace, and roughly half the video calls placed from our campus are now of the H.323 variety. Because no long distance charges accrue from an IP type call, a substantial cost savings can be realized from using H.323.

The History of Videoconferencing on Campus

Videoconferencing has come a long way since 1994, when it was first introduced at the UO. The days when the video quality of conference calls looked like "pictures from outer space" have all but disappeared. That annoying "delay" in the audio response has also been relegated to its place in history.

Gone—usually!—is the aggravating inability to connect with another videoconferencing site or the tendency for the video call to pixilate, freeze, or drop out entirely in the middle of a call.

This improvement in quality is largely due to better compression algorithms for both the audio and video signals, as well as the increased bandwidth now used for most calls. The vast majority of video calls these days are made at a bandwidth of at least 384 kilobits per second, making picture instability and audio delay a thing of the past.

Videoconferences can be point-to-point between two sites, or multipoint, joining as many as 24 sites on a voice-activated bridge. Up to four sites can be displayed simultaneously on video monitors using split-screen technology (also known as "continuous presence.")

In addition, media peripherals such as laptop computers and document cameras can be utilized to display hard copies of preprinted text and graphics or to share software applications. A very popular feature of the Polycom videoconferencing units is their ability to accept downloads of PowerPoint presentations so that all the participants in a video call are able to view the slides.

Current Videoconferencing Systems at the UO

There are currently eight video-conferencing systems being used by UO staff and faculty. These systems are in the following campus locations:

- Telecommunications Services (Rainier Building, Room 120)
- Media Services (Studio A in the Knight Library)
- Athletics Department
- OUS Chancellor's Office
- Department of Continuing Education (Baker Center)
- Computing Center (see **http://cc.uoregon.edu/cnews/winter2001/viewstation.html**)
- Knight Law Center

at the University of Oregon

The two systems available for general use by university staff and faculty are located in the Rainier Building and the Knight Library. In addition, every school within the OUS family of universities has video systems on their campus, as do most major universities.

The cost of a videconference (done from a Telecom Services videoconferencing unit) for university-affiliated personnel can vary depending on a number of factors, such as the number of sites participating and room rental rates at the far end, but the baseline cost is $80 per hour for the first hour and $40 per hour for each additional hour within the same session.

From a cost-versus-benefit standpoint, videoconferencing has earned a deserved reputation as a real money saver!

Setting up a Videoconference

In most cases, depending on the complexity of the call and the number of sites involved, a videoconference can be set up in a relatively short time frame (a 48-hour advance notice is usually sufficient) and reservations are taken on a first-come, first-served basis.

For additional information on the availability and pricing of videoconferencing, how you or your department might be able to incorporate videoconferencing into your university mission, or to book a videoconference, please contact Craig Leavy in Telecommunications Services, **346-1026**.

industry news

Microsoft's Competition with Linux Heats Up

On May 29, *The Washington Post* reported that Microsoft lost a contract with the city of Munich when that city opted to use Linux instead. Germany's third largest city isn't the only European municipality to lean toward Linux. And according to *The Seattle Post-Intelligencer, "*more than two dozen nations are considering proposals to promote or require the use of Linux in government offices."

References:

"Why Munich Dumped Microsoft for Linux"
http://www.eweek.com/article2/0,3959,1110813,00.asp

"Microsoft Loses Lucrative Munich Deal…"
http://www.usatoday.com/tech/news/2003-05-29-linux-munich-choose_x.htm

Apple Launches New 2GHz Power Macs

On June 23, Steve Jobs unveiled Apple's new G5 generation of Power Macs, calling them "the world's fastest personal computer" (a controversial claim, as demonstrated by the Slashdot discussions at **http://apple.slashdot.org/apple/03/06/28/1346251.shtml?tid=126&tid=181**)

The new machines, which have a 64-bit processor and can use up to 8 gigabytes of main memory, outpace both the fastest Pentium 4 and a dual-processor Xeon workstation in industry tests. They come in three versions: entry level (1.6GHz processor, 256 MB memory, 80GB hard drive, Nvidia GeForce FX5200 graphics card), midrange (1.8GHz G5 processor, 512MB memory, 160 GB hard drive, Nvidia GeForce FX5200 graphics card), and top-of-the-line (two 2GHz G5 chips, 512MB memory, 160GB hard drive, ATI Radeon 9600 graphics card).

More details about the G5, including an introductory video, are on Apple's website at **http://www.apple.com/**

Microsoft Drops Browser Support for Apple

Except for two minor upgrades, Explorer 5 is the last version of that browser Microsoft plans to develop for the Mac. However, Microsoft will continue to release Explorer 5 updates to address bugs and security problems. (See "Microsoft to Quit Web Browsers for Mac," **http://apnews.excite.com/article/20030614/D7RL7G280.html**)

Byzantine Legal Wrangle: Sun Tries to Capitalize on SCO Suit

In a bid to get royalties from any product based on Unix System V source code (including the AIX operating system), SCO is terminating IBM's AIX license and suing Big Blue for $1 billion.

Seeing an opportunity to increase its business in the licensing confusion, Sun Microsystems is urging users to switch from AIX to Sun Solaris.

For complete historical background on the SCO complaint, see the "Open Source Initiative Position Paper" at **http://www.opensource.org/sco-vs-ibm.html#id2854348**

Other references:

"SCO Owns Your Computer"
http://www.byte.com/documents/s=8276/byt1055784622054/0616_marshall.html

"Sun seeks to capitalize on SCO suit"
http://www.businessweek.com/technology/cnet/stories/1018669.htm

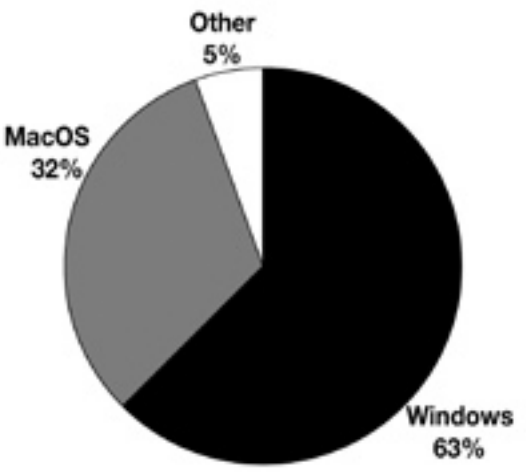
SP4 for Windows 2000 is Here…

For details on the newly released service pack, see
http://microsoft.com/technet/treeview/default.asp?url=/technet/security/news/w2ksp4.asp

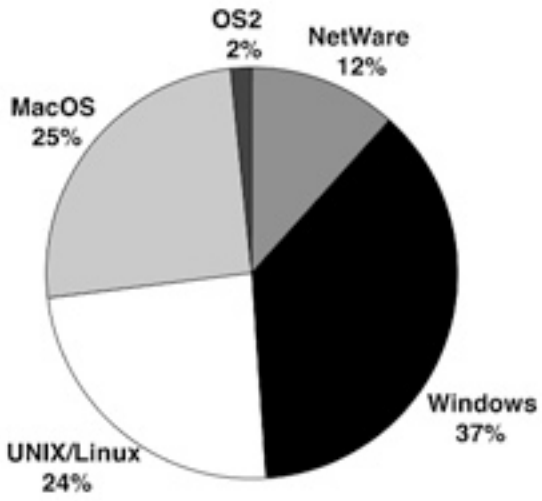
What Systems Are Currently in Use on Campus?

We recently conducted an informal poll among technical support staff on campus and came up with the following data. The poll was not strictly scientific, since not every department responded, but it does give a general idea of the distribution of desktop and server operating systems currently in use (excluding those in the Computing Center).

Desktop Operating Systems on Campus



Server Operating Systems on Campus



Departments May Request Spam-Blocking Exemptions for Role Accounts on Darkwing

If you are responsible for a departmental "role" email account* and if some of your important email correspondents have been inadvertently caught in the UO's spam-blocking net, there is a remedy: UO departments may request an exemption from spam blocking for their role accounts on Darkwing.

If you are interesting in having a role account exempted from our spam filters, please be aware of the following caveats:

- *Only* departmental role accounts—and of those, only accounts on *Darkwing*—can be exempted from filtering. *Individuals* who want a completely un-spam-filtered email address in addition to, or instead of, their spam-filtered UO account should create a supplemental account with a free email provider for that purpose. (We are not honoring requests for disabling spam filters for role accounts on Oregon because we're in the process of migrating all email accounts from Oregon to Darkwing. *Remember, all email accounts on Oregon will cease to exist in fall 2004. See article on page 11 for pointers to more detailed information about the migration from Oregon to Darkwing.*)
- Anyone requesting exemption from filtering for a role account should understand that this is a one-time-only, *permanent* election. We don't offer removal from filtering on a temporary/trial basis.
- If after disabling the filter you find that spam comes flooding into your role account, there's nothing we can do about it at that point. The problem then becomes your department's responsibility.

Contact: Departments who want to exempt their role accounts from spam filtering under this plan should contact Joe St Sauver (*joe@oregon.uoregon.edu*).

---

*A role account is a departmental email account that departments use for general contact purposes. Role accounts ensure that departmental email addresses remain stable over time despite personnel changes. Students or others with email questions about departmental policies or offerings are often routed to that central departmental mailing address (the role account) from a web page or printed mailer.

A Three-Year Effort Pays Off

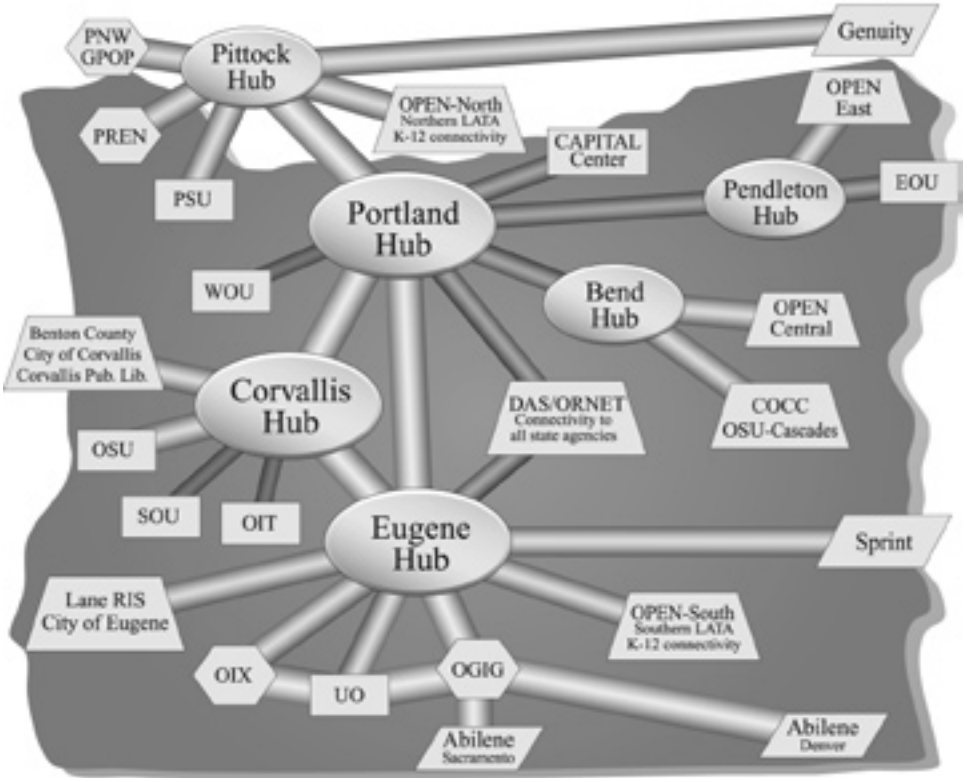
OWEN/NERO'S latest fiber project delivers information faster, cheaper

After three years of hard work, OWEN/NERO's latest regional fiber project was completed in December 2002.

OWEN (Oregon WidE area Network Partnership) and NERO (the Network for Education and Research in Oregon, based at the UO) collaborated on the project, working with local fiber consortia to expand and enhance the network backbone connecting Eugene, Salem, and Portland. Thanks to their efforts, and the labor of the Computing Center's Network Services staff, the backbone network operates at greater speed and at lower cost to its users.

Through the OWEN Partnership, public entities combine their network needs and can afford much higher speed connections than if each entity purchased services on the open market. NERO contributes the sophisticated engineering know-how to supply high-speed Internet access service to more than half a million K-12 students and over 100,000 students in higher education, as well as to all state agencies.

OWEN
(Oregon WidE area Network)



A map of the Oregon WidE area Network, showing the fiber path between partner networks. OWEN/NERO's latest fiber project added a Salem hub to facilitate faster direct connections between Eugene and Portland.

GET READY TO MIGRATE FROM OREGON TO DARKWING

Remember: by fall 2004 we will have discontinued service on Oregon, the academic VMS system. Now would be a good time to move your email and web pages off Oregon and onto Darkwing or Gladstone. For details, see:

- ***"Non-Administrative Access to OpenVMS on Oregon to Phase Out by Fall 2004"***
  http://cc.uoregon.edu/cnews/fall2002/oregonout.html
- ***"Migrating Mail from Oregon (VMS) to Darkwing or Gladstone (Unix)"***
  http://cc.uoregon.edu/cnews/fall2002/mailmove.html

Considering Setting Up Your Own

Try these tips for sharing Internet connectivity between multiple wired and wireless computers

Dan Albrich
Manager, Microcomputer Services
dalbrich@oregon.uoregon.edu

Although Microcomputer Services doesn't officially support home networks *per se*, we can give you some guidelines for making your home network setup as trouble-free as possible.

Note: Sharing your network connectivity between residences is generally prohibited. The sharing described here presumes family use within the same residence.

Who Should Consider a Home Network?

If you're already paying for a "broadband" high-speed DSL or cable modem Internet connection and have more than one personal computer in your family, it makes sense to have a home network. That way, everyone in your household can share the connectivity you're already paying for.

In some cases, a person may be paying for a DSL connection in one room of a house, yet routinely be dialing in via modem in another room of the same house. This is particularly inefficient because DSL also uses the phone line, and it actually reduces the speed and reliability of conventional modem connections. In addition, this type of setup also negates one of the best features of broadband connectivity, which is to allow Internet access without tying up a phone line.

If you have been limping along with the kind of inefficient setup we've just described, you'll definitely want to look into installing a home network.

What about Your ISP?

Okay, so you think you're ready to try a home network. The first thing to investigate is your Internet service provider's policy. Some ISPs make it easy to share the connectivity they sell you, and others make it difficult. Some may not allow you to share connectivity—even between your own computers at home.

If you use DSL, there is also a practical issue you need to consider: *make sure the provider gives you real Ethernet.* For example, Comcast cable modems have one connector for the coax cable, and Comcast provides a real RJ45 Ethernet jack so you can connect your home PC or almost any other Ethernet-compatible device.

The only ISPs we've heard of that don't allow this type of connection are the very-low-cost DSL options that give you an internal DSL modem and no external Ethernet connectivity. If you go with the DSL option, be sure to ask for an external modem and real Ethernet connectivity.

Methods of Sharing Your Connection

There are two ways of sharing your connection on a home network, only one of which is recommended:

1. Single IP Address Sharing *(Recommended).* With this method, you use NAT (network address translation) with dynamically assigned private addresses. To build a home network, you'll need to purchase a standalone device that combines the functions of a switch (sharing the physical connection) and also provides network address translation for IP address sharing. This method is not only less expensive than buying multiple IP addresses, it also helps secure your home computers from attacks. It's both easy and inexpensive to add wireless connectivity at the same time through a single device that serves both wired and wireless connections.

2. Multiple IP Addresses *(NOT Recommended).* Using this method, you would connect an Ethernet cable between your cable modem or DSL modem to a hub or switch, connect your computers to the switch via Ethernet cables, and purchase additional IP addresses for each computer.

Should You Enable Wireless?

Think of wireless network access as having the same properties as a wired network (like a hub without wires). To set one up, you need a base station that's hard-wired and a personal computer (usually a laptop) with wireless capability.

A variety of wireless base stations are available, with the best allowing both wired and wireless connections. For the sake of convenience, getting a single network-sharing device with both wired and wireless may make the most sense. Any network that includes wireless, however, will be more difficult to secure. For information on securing a wireless home network, as well as an overview of wireless standards and our recommendations, see our Home Networking page at **http://micro.uoregon.edu/homenetworking/**

Practical How-to Guides for Apple, Linksys: For basic information on setting up a typical home network with either Apple's Airport Basestation or a Linksys device, see the following pages on our website (your product version will likely not match these directions exactly, but the principles are the same):
http://micro.uoregon.edu/homenetworking/apple/
http://micro.uoregon.edu/homenetworking/linksys/

Home Network?

Important Restrictions On-Campus

Please do not connect a NAT box or other network sharing device (including one that supports wireless connections) without first asking permission from Network Services (**346-4395**, *nethelp@ns.uoregon.edu*). Network sharing devices typically come with a feature called DHCP for automatic IP address assignment turned on. DHCP is broadcast-based, and there should be only one DHCP server on a given network. Connecting one of these devices without first disabling the DHCP component can deny network service to other campus users. Introduction of private wireless access points may also interfere with official campus wireless service and is not generally permitted.

Basic Glossary of Terms

Packet: Data can be broken into distinct pieces or packets and then reassembled after delivery. Computers on the Internet communicate via packets.

IP address: Four numbers separated by periods, assigned to your computer. Having an IP address enables you to send and receive information.

Private IP address: Also called a nonroutable address, this is an IP address that's not generally reachable from external networks but is acceptable for internal communication.

Static Address: This is an IP address you purchase from your Internet provider that does not change over time. This type of address is the one you would typically want or need to run a server.

Dynamic Address: An IP address you purchase from your Internet provider that may change over time. DHCP is used to dynamically assign an address to your computer.

Globally Routable IP Address: This is a "normal" IP address in the sense that any computer in the world that's connected to the Internet can contact the computer having one of these IP addresses.

DHCP (Dynamic Host Configuration Protocol): DHCP enables a computer to automatically acquire an IP address on startup when connected to a network. DHCP uses broadcast, so it becomes important to have only one DHCP server on a network.

NAT (Network Address Translation): An IP sharing scheme in which one globally routable IP address is shared among several computers. Each of those computers is given a private, nonroutable address and the NAT device handles the translation. Most current home networking products use the term "router" to describe the ability to share a single IP address.

MAC (Media Access Control) address: Each network card has a unique hardware address. You can use this address to restrict access to only those computers with Ethernet addresses that match a list you supply.

Router: Routers select a path through the Internet so that a packet can reach its destination. "Router" is the term most often used by vendors to describe devices that share an IP address, although "network address translation device" would be more accurate in this case.

Hub: A simple device for sharing network connectivity. When a hub receives a packet on a designated port, it replicates that data to the other ports. In most cases, you'd be better served with a switching hub ("switch").

Switch: Also called a "switching hub," a switch reads the destination address of each packet and forwards it to the correct port. For this type of device, a switch is the thing to buy (as opposed to a hub).

AP or Access Point: This is a device that shares a wired connection with wireless clients. Think of an AP as a wireless hub.

Uplink: In satellite communication terminology, this term refers to the connection between the earth station and the satellite. On home network sharing devices, it's sometimes used to describe the connection between that device and the larger Internet (i.e., your DSL or cable modem). In the case of Linksys devices, the uplink port is either a standard port (for another device) or it can be used to connect another switch should you need more ports.

WAN Port (Wide Area Network Port): For Linksys devices, this describes the port to connect to your DSL or cable modem in order to connect to the larger Internet.

MDIX (Medium Dependent Interface Crossover): The label for the port you need to connect to the cable-modem or DSL modem. Think of it as the "uplink" for connection to the larger Internet.

SSID (Service Set Identifier): Also called "network name. Client computers must supply the network name to associate with a wireless access point. This can be used as a simple method to help keep unwanted users off your home wireless network.

WEP (Wired Equivalent Privacy): Encryption scheme used to protect wireless networks. Unfortunately, it is not very secure.

Who's Who at the

Meet some new members of our staff

Joyce Winslow
jwins@oregon.uoregon.edu

Dennis Vosika
Network Technician
Network Services

The latest addition to our Network Services staff is an energetic Oregon native who was born and raised in Medford, in an area still rural enough to inspire a lifelong love of the great outdoors.

Dennis Vosika might still be in his home town working as a contract electrician were it not for a series of events that began more than 20 years ago, when he married his wife Karen. Although Dennis and Karen had virtually grown up together, their relationship didn't really begin until long after their graduation from Medford High. In what can truly be described as a "happy accident," the couple became reacquainted after Dennis was injured in a serious motorcycle wreck. It took over six months for him to fully recover, and toward the end of his convalescence he called a cable company to order service. Coincidentally, it was Karen who answered the phone. The two quickly renewed their relationship and have been together ever since.

Dennis continued to work as an electrician to support his growing family, which soon included sons Trevor and Deven, but he was eventually lured north by the offer of more stable employment with UO Facilities Services, and the Vosikas relocated to the Eugene area in 1989.

Last winter, Dennis was persuaded to transfer his skills to the network arena, and he joined Network Services on December 1, 2002. Making the leap from electrical systems to network systems has required some adjustment, but Dennis is quickly getting up to speed. His first project was helping to update a Klamath science lab's network infrastructure, installing jacks and newer, faster cable. He's also worked on projects in Johnson Hall and is currently helping to get the network connections in the new Lillis Business Center ready for use next year.

For the past 14 years, Dennis and his family have lived the country life on 1.5 acres in Veneta with their "amazingly mellow" dog Will, a heeler/chow/lab mix, and cats Otter, Tippie, and Smokey. Trevor (now 20) and Deven (18) share their father's love of the outdoors, and hunting trips to Eastern Oregon are an annual father-son event. Once Dennis builds his new 1200 square-foot shop, the boys may also join him in his all-consuming hobby: restoring old cars. Recent restoration projects include a 1967 Malibu convertible and 1973 Chevy Nova. He's also busy collecting parts for a '62 Chevy pickup and has accumulated a grand total of five trucks thus far.

Laptop Lagging? Take it to the E-shop

If your laptop needs reviving, the Computing Center Electronics Shop can help.

Conveniently located on campus in 151 McKenzie Hall, the "E-Shop" offers extensive personal computer hardware support and repair services to UO students, faculty, and staff. Its technicians are experienced with many brands of microcomputers, laptops, and peripherals, including Apple and Windows/Intel machines, and can also offer advice regarding upgrades.

For more information, see
http://cc.uoregon.edu/e_shop.html

Computing Center

Cort Buchholz
Systems Analyst
Administrative Services

Cort Buchholz has already packed a lot of experience into his 26 years. He's been a student, entrepreneur, IT manager, systems analyst, rock band promoter, amateur musician, and bicycle racer—and for the most part, he still is all of these things.

Until the fall of 1999, Cort, a Portland native, was on track to get his Computer Science degree from the University of Oregon. But by chance, his work-study job in the Social Science Instructional Lab (SSIL) had introduced him to some fellow students who were members of a rock band called "16-Second Hum." Cort's own musical inclinations (he has studied both saxophone and guitar) and his enthusiasm for the band soon led to a connection with Paul Anthony, the founder of the pioneer digital music label "RumbleFish."

It was the heady era of entrepreneurial risk-taking and overnight success, and enthusiasm for startup businesses was at its peak. RumbleFish, with $125,000 in seed money from family and friends and the sponsorship of the UO School of Business, secured an office in the Riverfront Research Park, and immediately took off. Initially, the company focused on introducing new music in multiple genres, selling music downloads, and launching and nurturing new bands ("16" was one of its early protégés). In addition to "quasi-managing" his friends in the band, Cort took on the responsibility of being RumbleFish's IT manager and Chief Technical Officer, working with other technical consultants and student interns from the UO and PSU. Business grew so quickly, it wasn't long before Cort left school to devote his full-time energies to the fledgling company.

In August 2000, RumbleFish won the prestigious Angel Award in the annual Oregon Entrepreneurs Forum competition and was voted the number-one startup company in Oregon. Sensing it was time to expand, the company moved to Portland and Cort went with it. But while RumbleFish remained viable, it struggled in the sudden economic downturn. Needing a steady paycheck, Cort reluctantly bowed out to take a job as systems analyst with Integra Telecom. After 18 months with Integra, Cort began to think about finishing his degree. As luck would have it, a systems analyst position opened at the Computing Center just as he was ready to make his move, and Cort applied and was hired.

Now Cort is in his fourth month as an employee of Administrative Services and is picking up credits toward his B.S. degree, which he hopes to complete by the spring of 2004. His diverse real-world experience has served him well, both as a student and systems analyst. Cort's first major project at the UO is helping to launch Internet Native Banner (INB), which uses a browser-based interface. Other projects include Administrative Services' Network Security Initiative, upgrading DuckWeb, and implementing the UO's LDAP Directory Service.

NEED TECH TRAINING?

TRY DOCS ROOM'S WORKSHOPS-TO-GO

Visit the Computing Center's Documents Room (175 McKenzie Hall) and check out training CDs on Mac OS X, Win2K/XP, Excel, Flash—and more! For more information, see

http://darkwing.uoregon.edu/~docsrm/

Some Updates on Designing Your

New information on the way Excel and SAS communicate

Robin High
Statistical Programmer and Consultant
robinh@uoregon.edu

In the last issue of *Computing News* (**http://cc.uoregon.edu/cnews/spring2003/datadesign.html**), I described how to best design your data entry in Excel for transfer to a data analysis program like SAS or SPSS.

In the weeks since that article appeared, a few things about communication between Excel and SAS have surfaced, and the purpose of this article is to provide you with some pertinent updates.

Transferring Data from Excel to SAS

CSV and TXT files. One option I described was to create a comma-separated value (CSV) file or a tab-delimited (TXT) file of each individual worksheet, and then have SAS read these text files directly. (Before you save individual Excel worksheets as text files, be sure to save and back up your Excel workbook first, especially if it contains multiple worksheets. When you have finished exporting individual worksheets, exit the workbook without saving it.)

Whether you use Windows or Unix, you'll enjoy some advantages if you create CSV files with Excel and then read them directly with the SAS DATA step (or with DATA LIST in SPSS). It may not seem like this approach would be better than reading the Excel files directly, but it does have advantages if you have large data files, missing data, or inconsistently formatted columns. The DATA step allows you to read and format each variable, instead of leaving it to SAS to try to figure it out. How SAS does this is briefly described below.

Excel can also read comma- or tab-delimited text files directly, as easily as it can write them. By using CSV and TXT files, you will save on the time and disk space required to format every cell, substantially reducing the size of large files while ensuring that the file can be opened directly in either Excel or in SAS. However, keep in mind that problems can occur when importing text files into Excel that contain date variables or character data that Excel will interpret to be dates.

Close the Excel workbook before importing data. Before you attempt to run the PROC IMPORT statements or use the IMPORT wizard with SAS, you need to close the workbook in Excel first. For data integrity reasons, SAS and Excel aren't allowed to have access to the data at the same time. Even though you may have followed all the instructions correctly, SAS will give you an error message and fail to import the data if the file is still open in Excel.

Here are the statements for importing an Excel file into SAS:

```
PROC IMPORT DATAFILE="c:\<path>\test.xls"
 OUT=test DBMS=excel2000 REPLACE;
 SHEET="sequence";
 RANGE="A1:H20"; "A15:H35"
 GETNAMES=yes;
run;
```

Importing a portion of your Excel worksheet using the RANGE statement. One option I did not mention in my earlier article is that the IMPORT procedure allows you to read data from a specified portion of your Excel worksheet with the RANGE statement. It's not necessary to use this statement if you want to read the entire worksheet, but to specify only a *portion* of the worksheet, enter the range of cells between double quotes in a rectangular designation of upper left corner (A15) to lower right corner (e.g., H35), separated by a colon. This range assumes you have entered the variable names in Row 15.

If you are transferring one or more variables formatted as dates in Excel, SAS will read them correctly, but will save them with DATETIME formats (e.g., day/month/year/hour/min/sec) rather than a DATE (e.g., mm/dd/yyyy) format. This particular format may not work as you expect if you want to work only with the month, day, and/or year. To convert the date variable to a different format, use statements like the following:

```
DATA test1;
SET test;
DROP date;
FORMAT date_t mmddyy10. ;
date_t=DATEPART(date);
RUN;
```

Cell formatting. A common problem with either the import wizard or the PROC IMPORT statements is that if you haven't been consistent with cell formats in each column, SAS may get confused regarding the type of data it is actually trying to read. SAS scans the first 20 rows of an Excel worksheet to determine data types for each column. If for any particular column the first 20 rows contain all numbers (such as 3.3, 4.92, 2.0, 5, 3.1, etc.) or blank cells formatted as numbers, SAS will assign that variable a numeric format. If any data other

Data for Transfer into SAS

than numeric are read in that column after row 20, SAS will set the value of that row and column as missing in the dataset. However, if within the first 20 rows any non-numeric data are found (such as the characters 'NA,' 'M,' or a period for missing values) SAS will assign that variable to have a character format, even if the column is defined as numeric.

The number of rows SAS scans when determining data types can be modified from its default value of 20. There is an option called "guessingrows" which can be modified in the registry settings. For details on how to use this option, see
http://support.sas.com/techsup/unotes/SN/001/001075.html

Importing multiple Excel files. Suppose you need to import multiple Excel files with one worksheet and place them into one SAS dataset. And suppose these files have unique names like ab.xls, abc.xls, abcd.xls, etc., and you would like to import these files without writing their prefix names directly into multiple versions of the PROC IMPORT code. The corresponding SAS datasets should also be given the same names as the prefix of the Excel files. One solution is to create a list of file prefix names in a macro variable and then use a macro that reads each file listed in the macro variable. An example of this process is available at
http://darkwing.uoregon.edu/~robinh/data_transfer.txt

All the Excel files should be placed in the same directory. If they all have the same file structure and are to be appended to one another, this can be accomplished in one DATA file step with a SET statement that contains the same list of names from the recently created SAS datasets.

Exporting data from SAS *into* Excel

With all this focus on importing data from Excel, you may wonder if the reverse process is possible. Yes, there is both an EXPORT wizard and PROC EXPORT that work in an analogous manner to IMPORT. Exporting one SAS dataset to a single worksheet in a new Excel workbook is quite simple to do. However, EXPORT with version 8.2 is not as well-developed as IMPORT when working with multiple worksheets or transferring data formats. This will likely be a topic for a future article, especially when SAS 9.1, which includes features for efficiently exporting data into Excel, is released next year.

Network Security Team Expands Email Virus/Worm Defanging Ruleset for Darkwing, Gladstone, Oregon

SoBig.E virus outbreak prompts latest action

For the last several years we've blocked a variety of viruses, worms, and trojan horses by reversibly "defanging" potentially dangerous viruses (see the *Fall 2001 Computing News* article, "More File Extensions Defanged," at **http://cc.uoregon.edu/cnews/fall2001/defang.html**).

The emergence of the SoBig.E virus, which uses a zip attachment payload, has caused us to expand the set of file extensions that get defanged when emailed through Darkwing, Gladstone or Oregon.

Just like other potentially infective attachments, the two new extensions, **.zip** and **.zi**, will also be defanged by having the suffix **.txt** added to them.

What if you want to restore a legitimate zip attachment? If you receive a legitimate **.zip** or **.zi** file and wish to restore it to its original state, simply rename the file by removing the ".txt" extension that was added to the end of the filename. *But if you choose to do this, be careful!* Before making such changes, we recommend you verify that the sender intentionally sent the email message and attachment to you.

Security Alerts…

Microsoft Security Patch Has Bad Side Effect

Glitch affects Windows NT 4.0, NT 4.0 Server, Terminal Server Edition, Windows 2000, and Windows XP

Last April Microsoft released Windows XP SP-1, a hotfix for an "important" security flaw. The patch had what some described as "disastrous effects" on Windows XP, 2000, and NT 4.0 users because once installed, it slowed programs to a crawl.

Microsoft has since tried to address the problem by revising their guidelines for using the patch. See Microsoft Knowledge Base Article 815411: "Heap Algorithm Update for Atypically Large Heap Requests" at **http://support.microsoft.com/default.aspx?scid=kb;en-us;815411**

This latest bulletin explains that Windows XP SP-1 should be applied *only* to systems that are experiencing a specific, atypical problem. Those who are not severely affected by the memory problem the patch was designed to address are advised to wait for the release of its next Windows XP or Windows Server 2003 service pack that contains this fix.

Microsoft's Passport Flaw Puts 200 Million Accounts at Risk

In May, a flaw was discovered in Passport's password recovery mechanism that could have allowed an attacker to change the password on any account in which the username is known. Because the data frequently stored in Passport accounts includes such sensitive information as names, addresses, birthdates, and credit card numbers, a breach in Passport security leaves millions of users vulnerable to identity theft.

As soon as the flaw was discovered, Microsoft immediately turned off the vulnerable password recovery feature and replaced the service with a more secure version. Details on the Passport flaw, as well as Microsoft's plans to improve security in future versions of Windows, are available in Steven Musil's CNET News.com article, "Week in review: Red-faced Redmond," at **http://news.com.com/2100-1083-1000686.html**

Microsoft Moves into Antivirus Territory

In a bid to become a major player in the antivirus software field, Microsoft announced in June that it will buy antivirus technology from Romania's GeCAD Software and offer its own antivirus products.

Although Microsoft said it has no plans to bundle its virus software with Windows, most industry observers acknowledged the company has a strong competitive advantage.

More details on Microsoft's latest move are available in the IDG News Service report, "Industry wary of Microsoft's antivirus play," at **http://www.infoworld.com/article/03/06/10/HNvirusreact_1.html**

Microsoft Fixes Flaws in Its Internet Information Services Software and Windows Media Services

In May, Microsoft released a batch of patches to fix security holes in IIS versions 4, 5, and 5.1, which are all vulnerable to "cross-site scripting attacks." Additional patches were also issued to address flaws in IIS 4 and 5 that can lead to denial of service attacks.

At the same time, Microsoft released a patch that fixes a flaw in Windows Media Services for Windows 2000 and NT 4.0.

For more information, and to download the patches, see the following:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-018.asp
[Security Bulletin MS03-018: Cumulative Patch for Internet Information Service (811114)]

http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B817772
[MS03-019: Flaw in ISAPI Extension for Windows Media Services Could Cause Denial of Service]

AdSubtract Vulnerability

If you're using AdSubtract (a proxy server designed to block popups, animations, sounds, unwanted cookies, and the like), you should be aware that it may be vulnerable to abuse from external sources as an open proxy server due to incorrectly handled ACL checking. For details, see **http://www.net-security.org/vuln.php?id=2733**

Vulnerability in OpenSSH Daemon

Remote attackers have a better chance of accessing restricted resources because of a flaw in the way OpenSSH evaluates IP addresses and hostnames. For a complete description of the problem, including a list of affected systems and the recommended solution, see **http://www.kb.cert.org/vuls/id/978316**

Information Leakage Possible in Some Network Device Drivers

Network device drivers that reuse old frame buffer data to pad packets are vulnerable to remote attackers seeking to harvest sensitive information.This vulnerability may also affect link layer networking protocols other than Ethernet.

Network administrators are advised to use encryption to protect network traffic.

For full details, including a list of affected systems, see CERT's Vulnerability Note VU #412115 at

http://www.kb.cert.org/vuls/id/412115

New Release of SETI@home Corrects Buffer Overrun Vulnerability

A potential buffer overrrun vulnerability in versions of SET@home prior to version 3.08 has been fixed in the latest release of the software.

To get the software fix, download version 3.08 from the vendor's website at

http://setiathome.ssl.berkeley.edu/download.html

Worms in the News

Fizzer Worm. This complex new virus first surfaced on May 8, when it spread across the globe through email and popular file-swapping networks such as KaZaA.

The virus affects computers running Windows 95/98/ Me/NT/2000/ and XP. Its most worrisome feature is the key-logging program it installs on a victim's machine. This program has the capability to record everything you type into your PC, and can even record screen shots. Infected machines could expose such sensitive data as bank account numbers and passwords to malicious exploitation.

In addition to replicating itself through email, Fizzer also masquerades as a dummy media file in the KaZaA shared file folders of infected computers running P2P. Trademark file extensions of files containing Fizzer's executable code are **.exe**, **.pif**, **.com**, or **.scr**

To see Symantec's coverage of Fizzer, including removal instructions, go to

http://www.symantec.com/avcenter/venc/data/pf/w32.hllw.fizzer@mm.html

Effects of worms on Internet routing . The overall impact of worms on the Internet is well documented in Ido Dubrawsky's SecurityFocus article, "Effects of Worms on Internet Routing Stability" at

http://www.securityfocus.com/infocus/1702

Worms that forge headers. By now, most users are familiar with Klez-type worms that forge the "From:" header in email messages to disguise their origins (see *Summer 2002 Computing News* article "Worms, Worms, Worms..." **http://cc.uoregon.edu/cnews/summer2002/worms.html**).

The only way to definitively discover where the infested host *really* lives is by generating expanded headers and looking at the "Received:" lines. To find out how to do this, see the Microcomputer Services page at **http://micro.uoregon.edu/fullheaders/**

W32SobigE@MM Virus

Speaking of worms that forge 'From:' field headers...

This annoying virus has been seen on campus recently. It affects only Windows machines, and sends its infected attachment in a Zip file (often named "your_details.zip"). Look for a "Subject" line that is either "Re: Application" or "Re: Movie." (Note: Mac users may receive these same Sobig.E emails, but the virus can contaminate only Windows machines.)

The University of Michigan Virus Busters have some good information on this virus at

http://www.itd.umich.edu/virusbusters/sobig-e.html

Another Anti-Spam Product

CRM114, "the Controllable Regex Mutilator," is another spam product you might want to consider for your anti-spam arsenal.

The CRM114 system examines incoming email, system log streams, data files or other data streams, and sorts or filters them according to your specifications. It's compatible with Spam Assassin and other spam-flagging software and can be used as a syslog or firewall log filter.

One caveat: CRM114 is still experimental and without warranty of any kind. To find out more, visit the developer's home page at **http://crm114.sourceforge.net/**

Is Your Computer Safely Configured?

An America Online study reports that 89% of computers with broadband connections are not as safely configured as users think they are. For detailed study results, see **http://www.staysafeonline.info/press/060403.pdf**

The Economics of Spam: the Spam Business

Think spam is about selling actual products or services? Think again…

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

Even though the university blocks most spam on Oregon, Darkwing, and Gladstone, a trickle of spam will probably always slip through and annoy folks.

Any time we talk with people about that spam, someone will inevitably say, "Well, *someone* must be buying the stuff that's getting spamvertised, or spammers wouldn't keep sending spam, would they?"

That's an interesting thought, but an incomplete analysis.

It is true that spammers wouldn't keep sending spam if they weren't making money from spamming. But the *mechanism* by which they make money often has nothing to do with the sale and delivery of an actual product or service.

Spamming in an Effort to Grab Attention Online

Some spammers have a business model that lets them make money as long as people simply visit their website. You don't need to sign up for a spammer's online porn site, for example, because just visiting their publicly available website will be enough to ensure that the spammer gets advertising revenue from banner ads displayed on those pages.

This has an ironic implication: if you can convince people to click on an "unsubscribe" link (in a futile effort to stop getting spammed) you can make money from them the same way you would if they clicked on a web page for more information about a spamvertised product. We thus reiterate the recommendation we've made many times before: don't attempt to "unsubscribe" if you receive spam. If you do, you'll probably just end up with more spam, not less, and you may be putting money in some spammer's pocket.

You should also know that spammers who are relying on ad impression revenues will commonly put you into a linked series of pages—as you try to close one unwanted page, another unwanted page will pop up to replace it, thanks to Javascript. (Remember, we encourage you to configure your browser to run with Javascript disabled by default, although disabling Javascript may cause problems when you try to use some legitimate sites.)

Why do spammers take you from one unwanted page to another? Because every page they can force you to visit equals more ad impression revenues.

Fraudulent Spam: Relying on the Silence of Victims

In other cases, spammers make money by honest-to-god fraud. Is there anyone out there who hasn't received email asking them to URGENTLY HELP WITH THE CONFIDENTIAL TRANSFER MILLIONS OF DOLLARS IN OVERINVOICED RECEIPTS out of Nigeria?

Add to that fraudulent sweepstakes and lottery offers where no one ever wins (except the person perpetrating the fraud), various multi-level marketing/get-rich-quick schemes, online chain letters, and other types of fraudulent spam scams that have become so overused and hackneyed as to become almost laughable.

Other types of fraudulent spam are at least somewhat more subtle. For example, consider pump-and-dump stock tout schemes. These schemes attempt to "pump up" the value of a selected (fundamentally worthless) "penny" stock to astronomical levels, at which point the perpetrator can sell ("dump") that stock for a profit at others' expense. Although the Security and Exchange Commission (**http://www.sec.gov/**) does investigate and prosecute that type of stock fraud, their prosecution of a pump-and-dump fraudster may not result in recovering money you've lost.

In still other cases (particularly when a spammer is selling an "embarrassing" personal product or an illegal/quasi-illegal product, such as prescription medications without a prescription or cable descrambling devices), no one should be surprised when their check or money order is cashed but the promised product is never delivered (or, if some sort of product does get delivered, it fails to perform as advertised).

Spammers know, and rely on the fact, that their victims will probably be too embarrassed to contact the authorities to report that:

a) yes, they have been scammed, and moreover
b) yes, they were dumb enough to pay cash for magic penis enlargement pills—pills that were to be shipped from a company whose mailing address was a (now closed) PO box somewhere in Romania, and
c) yes, they did feel a need to buy magic penis enlargement pills in the first place...

Isn't Always What You'd Think

Or, consider the case of illegal/quasi-illegal products: if you order a satellite pay-per-view theft-of-service device from some person in Argentina and it never shows up (or it shows up but doesn't work), do you really think the police will be sympathetic and inclined to make your loss their top priority? Many authorities would be more inclined toward charging you with conspiracy to commit theft of television services!

If you want government help when you've been scammed, you need to come to the table with "clean hands" yourself. Don't let spammers con you into sending money to try to buy some illegal or quasi-illegal product or service.

"Pr0n Dialers"

Other spammers may make their profits by offering "free" access to online porn, with the only "minor" catch being that you need to use their "special software" to access that "free" site. In reality, the "special free software" is often a trojan horse, or a computer program that claims to be doing one thing while secretly doing something completely different.

For example, the "free special software" a "free" porn site may provide you could actually be using your modem to dial an expensive Caribbean 900-type pay-per-minute phone number without your knowledge or permission—until suddenly one day you get a phone bill for hundreds of dollars worth of calls made to some offshore destination. Good luck disputing those charges with the phone company!

Never load any software that a spammer or spamvertised website tells you you "need." Trust me, you don't need that software (or the pain it will bring you).

Serious Money

In other cases, the spammer isn't after just a few hundred bucks, he's really after your your name, address, credit card number, and credit card expiration date. Once he's got that information, he, or an accomplice, can then proceed to run up your credit card until:

a) he hits your card's credit limit, or

b) the credit card company discovers the fraud in progress and cancels your account, or

c) you get a bill for thousands of dollars worth of stuff you never purchased.

Fishing for credit card information this way is probably the single most common spam-related fraud on the Internet today, and is a prime reason why many businesses will no longer accept credit cards as a means of payment for orders shipped outside the United States or Canada, or will only accept credit cards for payment when the card's billing address and the order's "ship-to" address agree.

Your Identity

Other scamming spammers are playing an even more serious game: they don't just want your credit card information, they want your entire identity.

If a scammer can convince you to divulge your Social Security number and date of birth and private financial details such as your bank account numbers, perhaps as part of collecting information online for a "mortgage application," they can fundamentally destroy your financial identity.

Never provide detailed personal or financial information to any online entity that solicited that information from you via spam.

Making Money From Providing Spam Services

Other spammers make money through the sale of spam transmission software, and CDs full of addresses they've scraped from web pages, and lists of open proxy servers and lists of open SMTP relays. These guys sell spam support services to naive people who incorrectly believe that spamming is okay, or that spamming will result in a sudden surge in business and a financial windfall. This is somewhat like an advertising agency that makes money whether the products they help advertise actually sell or not.

Some of the world's largest telecommunication carriers are also among the entities making money from the sale of spam-related services. These carriers are perfectly willing to provide connectivity for spamvertised websites, for example, so long as the spam doesn't actually get sent from that connectivity (and with hundreds of thousands of open proxies out there, well, there's no need for a spammer to be that gauche!). Sales of high capacity transpacific and transatlantic OC3 and OC12 circuits to "strategic" customers are just too lucrative (and too potentially crucial to carriers teetering on the edge of bankruptcy) for those carriers to risk jeopardizing those revenue streams with trifles such as enforcement of an acceptable use policy!

So the next time someone tells you, "You know, spammers wouldn't keep sending spam if people weren't actually buying the stuff spammers were promoting!" step forward and tell them, "Hold on a minute! That's not true! Let me tell you a little about the economics of spam..."

Per-ASN DNS Blackhole Lists: the Latest Boon to System Administrators

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

The number and variety of DNS (domain name system)-based blacklists continues to expand. For example, ClueCentral.Net (**http://www.cluecentral.net/**) is now offering *per-ASN* DNS lists for all IPv4 address space known to be assigned.

What's an ASN?

An ASN, or "Autonomous System Number," is usually technically defined as a number assigned to "a group of network addresses, managed by a particular network operator, sharing a common routing policy." Most ISP and university networks have an ASN. For example, the UO's network uses AS3582; UC Berkeley uses AS25; Google uses AS15169; Sprint uses AS1239,… and so on.

Some large networks with particularly complex routing policies may have more than one ASN; others, with simple routing policies and only a single upstream network provider, may have none.

Bottom line, think of an ASN as a number that represents a particular provider or network.

What's a DNS Blackhole List?

The Domain Name System is normally used to efficiently translate a symbolic address (e.g., www.uoregon.edu) to a numeric IP address (or "dotted quad") such as 128.223.142.13. The DNS system can also be used in the reverse direction, taking a numeric IP address and returning the symbolic name associated with that dotted quad.

DNS blacklists use that same DNS infrastructure, but cleverly use it to return encoded information associated with a given network address of interest. That information might be whether or not a particular network address is associated with a dialup host, or whether a given network address is associated with a mail server that's known to be insecurely configured, or whether some other dotted quad is a chronic source of unwanted commercial email.

In this case, ClueCentral.net (the new ASN-oriented DNSBL mentioned earlier), allows a mail server administrator to check whether a given dotted quad is associated with an ASN of interest. For example, the DNSBL could be used to see if 128.223.142.13 is associated with AS3582 (it is):

```
host 13.142.223.128.AS3582.rbl.cluecentral.net
13.142.223.128.AS3582.rbl.cluecentral.net has address
127.0.0.2
```

If the specified address had *not* been associated with the specified ASN, the DNS system would have returned the message "domain not found," instead.

Why Would Anyone Be Interested in an ASN-oriented DNSBL?

Most ISPs, including the University of Oregon, have an acceptable use policy and enforce it, requiring their users not to spam or otherwise abuse other users of the Internet. Some ISPs, however, simply don't care and don't make any effort to deal with complaints about abuse their users engage in.

For example, let's assume that over a period of time, it becomes clear (via whatever mechanism) that the fictional ISP, Vladimir's Networked Borscht Shops (VNBS), AS91234, is overrun with spammers, and Vladimir really doesn't care (as long as the spammers keep paying and his borscht doesn't burn).

When that happens, other sites may decide they no longer want to accept any email from VNBS. Having reached that decision, they can then look up the network addresses associated with VNBS and use local filters to begin blocking all messages from those addresses. Using local filters that way can become tedious, since VNBS may add and delete network blocks over time, which means that the locally maintained filters will also require additions and deletions. You can probably keep up with a few providers this way, but if you're shunning traffic from several dozen (or more) entities, you'll need to peddle pretty hard just to keep up with the additions and deletions to those filters.

Enter the ASN-oriented DNSBL. Now, instead of having to look up and specify a set of network address blocks associated with VNSB, your mail administrator simply decides not to accept traffic from Vladimir's ASN, AS91234, and configures his mail server to use the appropriate per-ASN DNSBL zone for that ASN. Voila, he's done! …And, if the network addresses associated with that ASN change, those changes are automatically reflected in the per-ASN DNSBL.

Clearly this is a very powerful and convenient way for a mail server administrator to refuse unwanted traffic from a particular rogue ISP/ASN. Moreover, per-ASN DNSBLs are vastly preferable to the per-country DNSBLs to which some sites have resorted. Network abuse is not associated with *all* the network addresses assigned to *all* the networks in Brazil, for example, but rather with addresses assigned to a *particular ISP/ASN* (or set of ISPs/ASNs) which just happens to be in Brazil (or China, or the United States, for that matter).

Per-ASN DNSBLs do a nice job of matching consequences (e.g., filtering) with the parties responsible for the conditions which make that filtering necessary (e.g., tolerance of abusive customers and insecurely configured customer systems).

SUMMER WORKSHOPS

These information technology ("IT") workshops are free and open to currently enrolled students, as well as staff and faculty.

There is no registration; all seating is available on a first-come, first-served basis. **Unless otherwise indicated, prerequisites are required.** Requests for accommodations related to disability should be made to **346-1925** at least one week in advance of the workshop. For more information, contact the Office of Library Instruction (**346-1817**, *cbell@darkwing.uoregon.edu,* **http://libweb.uoregon.edu/instruct/**).

This schedule is subject to change. See **http://libweb.uoregon.edu/it/** for course outlines and the most current information, including answers to frequently asked questions (such as why you can't use your Oregon account in most of these workshops).

The fall workshop schedule will be available in late September.

Workshop	Day/Date	Time	Location	Presenter
Web Publishing, Multimedia ✔Prerequisites				
Web Publishing I - Learn how to create your own web page using HTML. ★✔***Prerequisites:*** Familiarity with a graphical web browser such as Netscape or Internet Explorer and an account on Darkwing or Gladstone (*not* Oregon!); you must know your username and password.	Thu July 10	2 - 3:50 PM	144 Knight Library	Frantz
	Tue July 15	2 - 3:50 PM	144 Knight Library	Nicholson
Web Publishing II - Introduction to cascading style sheets, diacritics and symbols, adding color and images, and more. ★✔***Prerequisites:*** Web Publishing I or equivalent knowledge and skills, and a web page you've created that's mounted on a web server or saved on disc.	Thu July 17	2 - 3:50 PM	144 Knight Library	Benedicto
	Tue July 22	2 - 3:50 PM	144 Knight Library	Munro
Web Publishing III - ★ ✔ ***Prerequisites:*** Web Publishing II or equivalent knowledge and skills	Tue July 29	2 - 3:50 PM	144 Knight Library	Bell
Dreamweaver I - An introduction to one of the most popular and powerful HTML editors currently on the market. ✔***Prerequisite:*** Web Publishing I & II or equivalent knowledge and skills	Thu July 24	2 - 3:50 PM	144 Knight Library	Nesselroad
Course Websites, Research Software				
EndNote/ProCite… Learn about the latest enhancements to these two programs, which are designed to help you organize and retrieve your citations and format your footnotes and bibliographies. You'll also learn how to connect to the UO Libraries Catalog and transfer citations directly into either EndNote or ProCite.	Tue July 15	12 - 1:20 PM	Science Library Seminar Rm	Zeidman-Karpinski
	Wed July 16	12 - 1:20 PM	Science Library Seminar Rm	Zeidman-Karpinski
Blackboard for Instructors - This fall we'll be offering a new version of Blackboard that has several new features as well as many changes to current features. Whether you're planning to use Blackboard for the first time this fall or you're an experienced Blackboard instructor planning to use it again, you'll want to join us for an overview of the new system and the ways in which you can use it most effectively.	Fri July 25	2 PM- 3:20 PM	144 Knight	Johnson
	Fri Aug 8	2 PM- 3:20 PM	144 Knight	Johnson

★ Requires an active account on Darkwing or Gladstone

COMPUTING CENTER GUIDE

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

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

Microcomputer Services
http://micro.uoregon.edu/

(151 McKenzie Hall)

- 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, $60/hour, 1/2 hour minimum)

346-4412
microhelp@lists.uoregon.edu

Documents Room Library
http://darkwing.uoregon.edu/~docsrm/
(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)

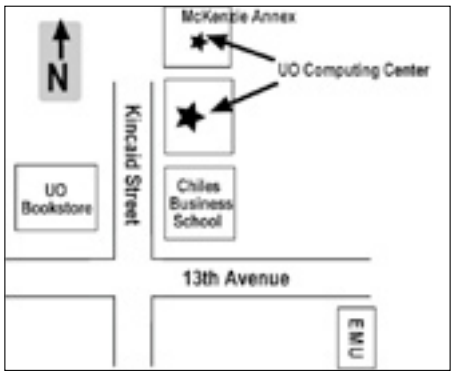
- VMS, Unix

(Gladstone, Darkwing, Oregon)

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

346-1758
consult@darkwing.uoregon.edu
consult@gladstone.uoregon.edu
consult@oregon.uoregon.edu

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



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

Network Services
http://ns.uoregon.edu/
Provides central data communication and networking services to the UO community.
346-4395
nethelp@oregon.uoregon.edu

Administrative Services
Provides programming support for administrative computing on campus, including BANNER, A/R, FIS, HRIS, and SIS. Call **346-1725**.

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. - 8:30 P.M.

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

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