University of Oregon

COMPUTING NEWS

WINTER 2002

IN THIS ISSUE...

Photo: Dave Ragsdale

Intel's donation of nearly $720,000 worth of 7340 and 7370 shaper boxes and e-Commerce Directors is a boon to network traffic management at the UO. See related stories on pages 5 ("Intel Donates Traffic Shapers") and 20-21 ("Understanding the Basics of Traffic Shaping," "How Load Director/SSL Accelerator Boxes Work").

Spam Blocking Improved on Oregon

New filtering mechanism should cut down the volume of unwanted email

Bob Jones
Senior Systems Manager
bj@oregon.uoregon.edu

In response to ongoing complaints from Oregon users concerning unwanted email, Computing Center systems staff recently broadened its spam-blocking efforts on the VMScluster to work the way they do on Darkwing and Gladstone.

The new filtering mechanism, which was activated December 17, enables us to block email from spam sites that had eluded our existing filters. Each of our filters has been instituted in response to complaints from one or more of our users—and usually a lack of responsiveness on the part of the administrators at the originating site when we notify them of the problem. In many cases the "From:" address in these messages is forged and does not correspond to a valid email address.

During our initial experimentation with these filters several months ago, we learned that a few users actually wanted to get messages from some of the blocked sites. To address their concerns, we're using a blocking mechanism that bounces the blocked message back to the sender. This should alert legitimate senders that their message didn't go through and enable them to contact their correspondent by other means (i.e., from a different address that we do not block).

If you discover you're not getting legitimate messages because they're being blocked by our filter, you have several alternatives:

1. You can ask your correspondents either to write you from a different email address, or have them ask their system administrators to contact *abuse@oregon.uoregon.edu* to try to resolve the problem. They should be sure to specify what domain they are representing, since ISPs will often serve numerous domains, not all of which we would be likely to block.

2. You can submit a request to *abuse@oregon.uoregon.edu* to remove a filter blocking a specific address, citing your reasons. We do not promise to honor your request, but we do promise to consider it carefully.

3. If we cannot justify removing our system-wide filter, we may be able to set up a personal bypass of the filter for your Oregon account.

UNIVERSITY OF OREGON

COMPUTING CENTER

COMPUTING NEWS

VOL. 17 #1

Computing News is published quarterly by the User Services and Network Applications staff of the Computing Center, 1212 University of Oregon, Eugene, OR 97403-1212.

© University of Oregon 2002

Contact:
Joyce Winslow
jwins@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

Photography: Dave Ragsdale

Got Extras?

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

Grayson Hall Renamed

The building that houses the Computing Center Annex is now known as McKenzie Hall

McKenzie Hall

The home of the Computing Center's Microcomputer Services, Computer Accounts, E-Shop, Documents Room, and computer labs now has a new name. At year's end, "Grayson Hall" officially became "McKenzie Hall," but only the name has changed.

Multimedia facilities and consulting help for a wide range of Windows and Macintosh dilemmas, as well as help with computing account passwords and computer hardware upgrades and repairs, are still available in Room 151 on the ground floor of the building. You'll find the Documents Room library, with its ever-expanding collection of books, magazines, and instructional CDs and videos, down the hall in Room 175; and the Computing Center's computer labs are still in Room 101.

The Social Science Instructional Labs (SSIL) are also located in McKenzie Hall, upstairs in Rooms 442 and 445.

Until we update all our publications, you may still see references to "Grayson Hall," but don't let that confuse you. All of our Computing Center Annex services are still available in the old familiar places.

Campus AppleTalk, Novell IPX Connections to be Completely Phased Out in 2002

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

As many campus departments are already aware, Network Services has begun phasing out AppleTalk and Novell IPX network routing on campus. By July 1, the entire campus network will have migrated to TCP/IP-based service.

The only noticeable effect this changeover will have is to limit AppleTalk and Novell users to their local (e.g., in-house) servers. Usually these subnets are in a single building. Unless you employ TCP/IP-based services, users outside your building or subnet will not be able to log onto your fileservers or print to your printers.

TCP/IP-based services are available for both Novell (Windows) and AppleTalk (Macintosh) systems. To use them, you'll probably need to reconfigure servers and desktop computers. You'll also need to be sure you have current software. (The minimum software version for Novell to enable TCP/IP services is 4.0, but version 5 is recommended. The minimum version of MacOS is 8.6.)

Phase-Out Schedule:

November 1, 2001: The UOnet zone was removed from all AppleTalk networks.

January 1, 2002: Novell IPX routing on campus core routers was turned off. Novell IPX routing was provided to a very limited set of buildings.

July 1, 2002: Novell IPX services and AppleTalk services will be turned off campuswide.

Remember: Unencrypted Telnet Eliminated January 14

Rick Millhollin
Director of Computing Facilities
rickm@oregon.uoregon.edu

As of January 14, you will no longer be able to use telnet to connect to Darkwing, Gladstone, Oregon, Daisy, or Donald. If you attempt to use telnet instead of secure SSH software, for now you'll see the following error message:

```
CAUTION! This telnet connection is unencrypted and hackers/crackers may be able to eavesdrop upon your username and password and other network traffic. Because of this vulnerability, unencrypted telnet access to the VMScluster (or Gladstone and Darkwing) will be discontinued effective January 14, 2002.
```

Hopefully, most telnet users of these large-scale Unix and VMS systems have by now seen the advance expiration notices displayed online. Telnet's demise was also publicized in last summer's *Computing News* ("Time to Begin Using SSH," **http://cc.uoregon.edu/cnews/summer2001/ssh.html**).

Free SSH clients for your PC or Mac are available on the UO Duckware CD-ROM. The Duckware 2001 CD, which was released in September, automatically activates the SSH installer when you insert it in your machine. After the installation is complete, Mac users will find SSH by going to the Apple Menu -> UOnet -> Telnet -> Better Telnet. Windows users will find the SSH links under Start -> Programs -> Network Applications ->Telnet (SSH).

If you need help installing SSH, see the Microcomputer Services security information page at

http://micro.uoregon.edu/security/

or contact *microhelp@oregon.uoregon.edu* (**346-4412**).

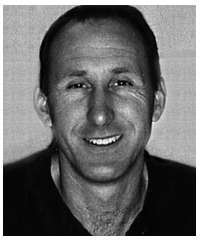
Sony Donations Enhance UO's Digital Video Capabilities

The University of Oregon would like to thank Sony Corporation for its generous donation of video acquisition and editing equipment, which will greatly enhance the digital video capabilities of UO faculty, staff, and students.

The new equipment includes a digital video camcorder for acquiring video and still-shot images and two laptops for editing and translating the resulting digital files. One of the laptops will be used for translating and editing content from various network sources, and the other, for capturing images and video content from the digital camcorder.

The new equipment will soon be available for checkout for special projects from the Computing Center. Watch for details in the next edition of *Computing News*, or call **346-4412** for more information.

Campus Wireless Network Update



The new system will be more reliable and easier to use, and coverage will continue to expand

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

Beginning the week of February 4, 2002, Network Services will begin converting the existing wireless network to a simpler and more reliable system.

The new system will allow you to use any 802.11b card and requires only that your device have appropriate drivers for 802.11b, a DHCP client, and a web browser that supports SSL (Secure Socket Layer) encryption.

To use the campus wireless network, simply install the wireless card and open a web browser to any URL. You'll automatically be redirected to a web page that requests your username and password (the same username and password you already use to connect to the campus network). After you're authenticated, everything will work as you'd normally expect.

Encryption. Note that encryption will no longer be provided by our wireless network, so be sure to use SSH and SSL-based services!

Network coverage. Network Services is continuing to expand wireless coverage on campus. Watch for announcements of new coverage areas in future issues of *Computing News* and online at **http://micro.uoregon.edu/wireless/**

Questions? For up-to-date information about the UO's wireless network, including system requirements and detailed instructions for getting connected, see **http://micro.uoregon.edu/wireless/**

All New Macs Ship with MacOS X

MacOS 9 'Classic' mode remains available

As of Monday, January 7, all new Apple Macintosh computers began shipping with MacOS X, Apple's next generation operating system. However, Apple will continue to install the prior operating system, MacOS 9.2.2, so that users can run software in Classic mode if they wish.

This configuration is similar to prior configurations except that MacOS X is set as the primary operating system. Users may still restart in MacOS 9 if they wish.

To boot into MacOS 9 from MacOS X, select "System Preferences..." from the Apple menu and click "Startup Disk." Click the MacOS 9 folder that appears in the list and then click the "Restart" button to reboot into MacOS 9.

To learn more about MacOS X, go to **http://www.apple.com/macosx/**

Apple Unveils New iMac

Joyce Winslow
jwins@oregon.uoregon.edu

Apple's new flat-panel iMac was the big news at this year's Macworld trade show in San Francisco.

Although Apple founder and CEO Steve Jobs unveiled a suite of other new and enhanced products, including a new 14-inch iBook with a DVD-ROM/CD-RW combo drive, iPhoto software that magically manipulates digital photos, and the iPod music player, the new iMac captured most of the headlines.

Continuing the emphasis on innovation that has been Apple's hallmark in recent years, the new all-in-one iMac is a radical departure from conventional desktop computer design. This futuristic model, which resembles a swing-arm lamp with its slim 15" liquid crystal display screen attached by a jointed chrome bar to a rounded white base, sports a G4 processor and SuperDrive for playing and burning both CDs and DVDs.

The new product reflects Jobs' vision of the personal computer as a "digital hub," the central unit from which all other digital devices radiate. Following this concept, the new-era iMac is designed to simplify your life by orchestrating the functioning of such devices as camcorders, digital cameras, and MP3 and DVD players.

A full description of current Apple products and features, including links to reviews of the new iMac, are online at **http://www.apple.com/**

@Home's Demise Creates Cable Modem Woes

The rocky road for cable Internet users isn't over yet

Dan Albrich
Microcomputer Network Specialist
dalbrich@oregon.euogon.edu

Eugene cable modem users lost service on December 1 when the Internet provider @Home stopped its service due to financial problems.

Some users may have hardly noticed the brief outage because AT&T created a backup network to provide service. The big problem is that all of the former @Home users had to change email addresses and may have lost prior emails stored on the @Home system.

While AT&T hasn't raised the price of cable Internet service, it has reduced the speed of downloads to less than one quarter their former maximum. Cable users in Eugene can expect to get no more than 1.5Mbps for downloads and no more than 128Kbps for uploads.

What about DSL? Comparably priced DSL service includes 640Kbps for downloads and 256Kbps for uploads. The uploads are faster with DSL, but the downloads are limited to less than half that of cable. Since most home users are most concerned with download speed, cable Internet service is still quite reasonable.

Unfortunately, the rocky road for cable Internet users isn't over yet. On December 20th, AT&T announced a merger with Comcast to form a new company called "AT&T Comcast." The new company may or may not change services and prices for cable modem users. This type of change can reduce the quality of the service, raise prices, or both. We'll hope for the best until the facts are known.

Occasional DNS Problems with UO Systems. Cable modem service in Eugene has not been perfect. A minority of users have suffered a major problem with Domain Name System (DNS) registration both under @Home and AT&T's new management. (DNS is a table of names that map to IP addresses. Its converse, "reverse DNS," maps IP addresses to names. For example, DNS tells Internet users that darkwing.uoregon.edu is at 128.223.142.13, while reverse DNS would let someone curious about the name of 128.223.142.13 find out that it points at darkwing.uoregon.edu.)

Internet providers are obligated to provide DNS registration for basic Internet connectivity. In a number of cases, cable modem users lacked either forward or reverse DNS entries—effectively disabling their connections to our timesharing hosts Gladstone, Darkwing, and Oregon, all of which require correct DNS registration. (We require proper DNS registration for incoming connections because computers that have incorrect registration are often used intentionally by spammers or hackers to try to conceal their identity.)

In the past, users affected by this DNS problem have had great difficulty reaching either @Home or AT&T to get the problem resolved. @Home had a policy against users running any server software in their home over the cable modem connection. The new AT&T network takes that a step further by blocking certain inbound connections. For example, AT&T currently blocks all inbound port 80 connections so it is not possible to run a web server on the standard port from home. This isn't a change in policy, but a change in the level of enforcement. (For more details regarding AT&T's Internet acceptable use policy, see their information page at **http://help.broadband.att.com/faq.jsp?content_id=1107&category_id=34&lobid=1**)

At the moment, Microcomputer Services is unaware of anyone encountering DNS problems, but past experience requires us to mention them for your consideration.

If you're a current cable modem user and are happy with the service, you may want to stick with it. Cable modem users pay month-to-month without a contract, whereas all current DSL promotions require a one-year agreement. On the other hand, if you're considering a new cable modem purchase you might want to wait until the effects of the Comcast merger are known.

UO Public Safety Offers Laptop Security Devices at Discount

If you're interested in protecting your laptop or other valuable electronic equipment, you'll probably want to investigate S.T.O.P. security plates. S.T.O.P. is a highly effective theft prevention tracking system that imprints your equipment with a scannable bar code and uses an international registry for recovery.

The UO's Department of Public Safety is now selling S.T.O.P. at cost to UO students, faculty, and staff. You can purchase the plates, which normally retail for $25, for $17.50 by going to the Public Safety office at 1319 E. 15th Avenue, diagonally across the street from the Student Recreation Center. For more information on this program, call **346-5444**. More information about S.T.O.P. is online at **http://www.computersecurity.com/stop/**, and the address for the International registry and product site is **http://www.stoptheft.com/**

Windows Users: Having Problems with Duckware 2001? Try These Solutions…

Dan Albrich
Microcomputer Network Specialist
dalbrich@oregon.uoregon.edu

After the Duckware 2001 CDs were released last fall, some minor software problems came to light. A bug in SSH.COM's SFTP client v.4 caused permissions errors, Norton AntiVirus 2002 wouldn't install on Windows 95 (see "Watch for Norton AntiVirus Live Update Problems" on page 7), and some users had trouble finding the documentation.

If you're having any of these problems, try the following suggestions:

1. SSH/SFTP v2.4 Problem: There is a known permissions umask problem with SSH.COM's SFTP client v2.4 that's included on Duckware. Because of this glitch, if you drag an HTML file onto your PC, edit it, and then drag it back, others may not be able to view that web page.

Solution: After Duckware was distributed, SSH.COM issued a fix for this bug. All you need to do is install the SSH.COM package *build203* directly over v2.4—no need to remove the old version. The new version obeys the permission umask by default, and allows global permissions to be assigned in the preferences screen if you always want to assign a particular set of permissions. To download this patch, go to

http://micro.uoregon.edu/security/dist.html

and click on the "Windows" link under "SSH (Telnet replacement)."

2. Windows 95/Norton AntiVirus 2002 Problem: Norton AntiVirus 2002 will not install on Windows 95. It will, however, automatically launch and install NAV 2001 on Windows 95B and higher machines after notifying the user.

You can get LiveUpdate codes at **http://micro.uoregon.edu/av/** These codes allow older versions of NAV to continue to receive live updates of current virus definitions. One caveat: If Symantec releases a new version of NAV next year as expected, NAV 2000 will no longer work for live updates. (In some cases, installing IE SP2 on Windows 95 will upgrade system components to a level where newer software can work. This might be worth a try for advanced users.)

3. Problems Finding Documentation: Documentation is not automatically installed when you insert the Duckware CD unless you choose the "Easy" NetApps Install option, which creates a desktop shortcut called "UO Duckware Start Here!"

To read the documentation without installing it, look for the "documentation" folder and double-click on the file "index.html".

Some Sites Worth Investigating…

Whether you're an electronics buff, a systems administrator, or a Linux fan, here's a sampler of sites that may pique your interest:

1. **Hop-On Communications.** Got a yen for a disposable, recyclable cell phone? Check out **http://www.hop-on.com/**
2. **Windows 2000 TCP/IP Performance Enhancements.** This service pack offers enhancements included as a hotfix for Windows 2000: **http://support.microsoft.com/default.aspx?scid=kb;en-us;Q298896**
3. **Novell Client Software Enhancement.** See the list of resources at **http://www.ithowto.com/novell/clientspeed.htm**
4. **Quick Guide to LDAP.** This site covers everything from theory to the niceties of configuration and also offers useful links to related information and downloads: **http://k12linux.mesd.k12.or.us/ldap/index.html**
5. **Executive Order on Critical Infrastructure Protection.** The full text of President Bush's IT security directive is online at **http://www.whitehouse.gov/news/releases/2001/10/print/20011016-12.html**

Watch for Norton AntiVirus LiveUpdate Problems

Tips for solving common problems

Spencer Smith
Microcomputer Support Specialist
spencera@oregon .uoregon.edu

Several bugs associated with Norton AntiVirus (NAV) LiveUpdate have surfaced in recent months. These bugs primarily affect Windows users, and, while troubling, have fairly simple solutions. We've outlined some of the main problems and their remedies in the paragraphs below:

Windows 2000 and NAV 2002 Problems. Some Windows 2000 users have reported problems installing Norton AntiVirus 2002 when an earlier version of NAV is already installed on their system.

In some instances the installer freezes, asserting that access to a Registry key could not be modified. Another bug shuts down Win2K users who have Promise ATA Ultra66 disk controllers and NTFS formatted system partitions.

This problem arises because Windows handles streaming data as a special file, and with NTFS it treats these files like any other file. When the data is streaming, the file never reaches an "end-of-file" mark and NAV continues to scan it forever, resulting in an increased process load and eventually grinding the computer to a halt.

Solution: If you're experiencing either of these problems, you can get the patches and documentation from Symantec's technical support page at

http://www.symantec.com/techsupp/files/lu/lu.html

All you have to do is install the update and reboot the computer. Once your computer restarts, run the LiveUpdate program and allow it to update all your Norton AntiVirus components.

Windows 95 Problem. Some users complain that Norton AntiVirus notified them that their LiveUpdate subscription had expired. They were then prompted once for the LiveUpdate subscription code, but if they clicked "Cancel," they were unable to get the prompt to reappear. In addition, LiveUpdate ceased to function because of the expired subscription.

Solution: For directions on entering your subscription key, see Symantec's technical support page at

http://www.symantec.com/techsupp/subscribe/directions/

Here you'll find illustrated, step-by-step directions for almost all versions of NAV for both PC and Macintosh.

UO computing account holders can get the current subscription code from **ftp://public.uoregon.edu/software/AntiVirus/update.txt**

If neither of these methods is effective, you may need to download a newer version of LiveUpdate from Symantec and install it. You should also check your date and time control panel and make sure the settings are correct.

"LiveUpdate could not get the list of updates…" Error Message. Some users may see this message after they activate LiveUpdate. The initial message is followed by the comment, "LiveUpdate could not retrieve the catalog of available Symantec product updates. Please check that your connection to the Internet is functioning correctly and retry LiveUpdate."

Solution: There are several reasons why you may get this message. To troubleshoot the problem, go to **http://www.symantec.com/search** and search for the phrase **"LiveUpdate" and "error message"** Scroll through the list until you find the specific error message cited above.

Beware of Passport Perils

Leaving yourself open to identity theft is among the hazards of using Microsoft's "single identity" authentication system

Joyce Winslow
jwins@oregon.uoregon.edu

Last fall, we reported the vulnerability of Microsoft's Passport authentication program to Trojan Horse viruses (see "Watch Out for Microsoft Passport Security Woes," **http://cc.uoregon.edu/cnews/fall2001/passport.html**).

Now identity theft has been added to the list of Passport liabilities by Seattle researcher Marc Slemko. Slemko pinpointed the weakness by devising a Hotmail exploit that steals Passport authentication cookies and impersonates the victim (for details, see **http://alive.znep.com/~marcs/passport/**).

Passport is still used primarily for Hotmail accounts and customizations on other Microsoft sites, so relatively few UO users are currently at risk. However, as Slemko points out, if Passport authentication becomes more widely used, the security implications of having a single identity for a user across the Internet are far more grave.

Take Advantage of the UO's Expanding GIScience Resources

UO students, faculty, and staff may now check out hand-held GPS units as well as ArcInfo, ArcView and ArcGIS media to load onto their work or home computers

Aileen Buckley
Assistant Professor, Geography

Hans Kuhn
Computing Center User Support Specialist

Whether you're researching the biosphere, studying global environmental change, or designing a transportation network, Geographic Information Science (GIScience) applications are invaluable aids. To keep pace with the demand for sophisticated geographic information technologies, resources supporting GIScience at the University of Oregon have increased dramatically in recent years.

GIScience—which involves the collection, management, analysis and display of spatial data—employs technologies such as geographic information systems (GIS), global positioning (GPS), remote sensing, cartography, and geographic visualization.

GIScience figured prominently in such notable projects here in the Pacific Northwest as forecasting salmon populations, projecting the effects of various forestry practices, supporting disaster management in the wake of landslides, earthquakes, and floods, and predicting climate change relating to El Niño. Most recently, GIScience tools were used in the production of *The New Atlas of Oregon*, which highlights the work of UO geographers.

A major milestone in building the UO's GIScience resource base is a statewide site license, organized by the UO, which provides all OUS campuses and ten community colleges with unlimited ESRI GIS software. This license enables UO students, faculty, and staff to check out ArcInfo, ArcView and ArcGIS media from the Computing Center's Documents Room Library in 175 McKenzie Hall and load the software onto their work or home computers. In addition, anyone at the UO may now learn about the software and its applications by taking courses from the ESRI Virtual On-line Campus at **http://campus.esri.com/**

Other GIScience resources include a site license for new ERDAS remote-sensing software, as well as ten hand-held GPS units that can be checked out from the Social Science Instructional Lab (SSIL) in 460H McKenzie Hall. Both these resources were obtained through a grant written by the Geography Department and SSIL faculty.

This funding also supported the development of a set of online teaching modules that were designed to introduce people from all disciplines to the basics of GIS, remote sensing, and GPS. These modules, which include written descriptions and hands-on learning exercises, are available from the SSIL web page at **http://ssil.uoregon.edu/gis/NWACC/NWACCIntro.htm**

The modules can be used to supplement courses in which the acquisition and use of geographic data is helpful, and to teach faculty, students, and staff to become more proficient in the use of these technologies.

Now that these new resources are widely available, it is hoped that GIScience tools and techniques will be incorporated in an increasing number of disciplines and activities across campus.

For more information about GIScience resources on campus, please contact Hans Kuhn at **346-1714** or email *hak@oregon.uoregon.edu*

Get GPS Info from A to Z at joe.mehaffey.com

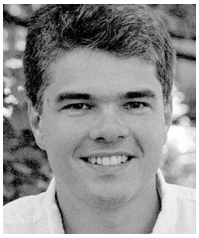
Whether you're a new user of Global Positioning Systems or a seasoned GPS enthusiast, you'll find something of interest on Joe Mehaffey and Jack Yeazel's GPS Information Website at **http://joe.mehaffey.com/**

The site includes a newsgroup, product reviews, and tips for GPS fans, as well as dozens of links to PDAs and laptops, more GPS products and accessories, and other GPS information sites.

One caveat: Before visiting this site, you may want to turn Java off in your browser to avoid the many pop-up windows it generates.

Tips for Avoiding Common Email Pitfalls

Take a moment to review your email habits before hitting the "Send" button



Patrick Chinn
Distributed Network Computing Consultant
Microcomputer Services

Electronic mail is now a common form of communication, yet many email users are unfamiliar with some of its common pitfalls. The unfortunate mix of unsophisticated users and sophisticated email software can result in unreadable messages, clogged servers, and possible embarrassment.

This article describes some of the most common email problems we see at the university and offers suggestions for avoiding them.

File Attachments

Files attached to email messages have the potential to cause a variety of problems, including:

• **Size:** Attachments can be large and fill the recipient's inbox, blocking the receipt of future messages. To prevent users from filling another person's account, we limit the size of file attachments to 2MB or less.

• **Readability:** Some attachments can't be opened and used by the recipient.

Before sending a file as an attachment, contact the recipient to see if he or she can handle that type of document. Avoid sending attachments to large mailing lists (see "Mailing lists" below). A possible solution: cut and paste just the contents of the file into the body of the email message itself.

• **Mailing lists:** Sending a large attachment to a large number of recipients, either through a private list or through a listserv, can cause network delays or failures as the server attempts to process the data.

• **Computer viruses:** If your computer is infected with a virus, you may infect those who open email attachments you send. To avoid this problem, don't send files as attachments and use antivirus software.

Alternatives to email attachments do exist. If many people need access to a file, put the file itself or the contents of the file on a web page and email the web page address to the group. Darkwing, Gladstone, and Oregon email accounts can be used to host web pages. For more information on how to host a web page, see **http://cc.uoregon.edu/documents.html**

HTML-Formatted Messages

Email messages formatted using HTML (the format used to create web pages) are often unreadable by recipients. The key to using HTML email successfully is to know your audience. Before sending an HTML-formatted message, ask yourself, "Do I know for certain that the recipient(s) can read this message?" If the answer is no, use plain text.

Regrettably, several email programs format messages with HTML by default. Microsoft's Outlook and Outlook Express are the most common culprits. (The default can be changed. In Outlook XP, go to Tools -> Options ->Mail Format and select "Plain Text." In Outlook Express 6 go to Tools ->Options ->Send and select "Plain Text.")

Reply to All

When replying to an email message, double-check the address to which your reply will be sent. Users embarrass themselves daily by sending replies to a group or a list rather than the specific individual. Checking the email addresses on your reply before clicking the "send" button can prevent possible mortification. (Generally there is no way to recall or delete a message once it has been sent.)

"Me Too"

Avoid the temptation to reply with nothing more than "me too." If a reply is necessary, snip out some or most of the original email message, leaving only the pertinent question or statement. This saves bandwidth.

Off-Topic Messages

When posting a message to an email list, ask yourself, "Does the topic of my message fit the subject or scope of this email list?" If not, find a more appropriate forum. At the minimum, state at the beginning that your message is off-topic.

Vacation Messages

Some people use the "vacation" program when they are out of the office. (When a new message is received, the server automatically sends a "Sorry, I'm out of the office until next week" message.) This feature is especially troublesome if you are subscribed to a list because your vacation response may be sent out each time you receive a message from that list. A user subscribed to a busy list could easily generate a hundred or more vacation messages to a group of people who do not care that you are vacationing in Atlantic City until Thursday. We recommend unsubscribing yourself from email lists before leaving on vacation.

Note: The vacation program is available only on Darkwing and Gladstone. It is not available on Oregon.

Conclusion

Taking a moment to review your email habits before hitting the "Send" button can save you, and those on your mailing list, a lot of grief in the long run.

NWACC Proposals Due March 15

Guidelines and online application forms for Northwest Academic Computing Consortium grant proposals are now available at **http://www.nwacc.org/grants/index.html** Applications must be received by 5:00 pm PST, March 15, 2002. For eligibility codes, contact Joanne Hugi (*hugi@oregon.uoregon.edu*).

New Windows XP Offers Mixed Bag of

New version combines consumer and business operating systems

Dan Albrich
Microsoft Network Specialist
dalbrich@oregon.uoregon.edu

The Windows XP operating system started shipping on new computers in late September and was officially released in late October. This new version of Windows combines Microsoft's consumer and business operating system versions into one core Windows product. The prior *consumer* versions of Windows, which were made for home use, include Windows 95, 98, and ME. The prior *business* versions of Windows include NT and 2000.

Some of us remember the "Designed for Windows 95" logos on software from the past. This logo often meant the same program would not run on Windows NT. What made this distinction even more problematic is that many "Designed for Windows 95" programs actually would work just fine under NT, but ultimately you'd have to install the product to know for sure.

Such confusion is now eliminated, as Windows XP will essentially be the same product for both business and home users. While bundled software and some capabilities will vary between the Professional edition (which is aimed at business users) and the Home edition, these are largely marketing decisions and not technical limitations. The advantage of the unified XP version of Windows is that software designed for XP should work equally well on either the Professional Edition or the Home Edition unless it was specifically designed not to work on both.

Some Things to Watch Out For

The big "gotchas" with Windows XP—activation, .NET passport requirement for some services, lack of password requirements, and hardware compatibility issues—are summarized below:

Activation. The most controversial aspect of the new Windows version is a requirement called activation. Activation is designed to stop software theft. The "off the shelf" copies of Windows XP all require activation, either over the Internet or by calling Microsoft. If users wish to install the product on a different PC later on (i.e., move the license) or if they make too many changes to their hardware configuration, they are also required to call Microsoft.

Departments ordering with a purchase order can avoid activation completely by purchasing the XP product through OETC (Oregon Educational Technology Consortium, **http://www.oetc.org**) or the UO Bookstore (**http://www.uobookstore.com**). OETC can order individual copies, whereas the Bookstore requires an order of five copies or more.

.NET Passport. MSN Instant Messenger, included with Windows XP, now requires users to sign up for a .NET passport. This is a single username and password that enables logins to multiple web sites. While Microsoft promotes this as a convenience, we recommend extreme caution when putting personal information into any website or service, and especially those that store financial information about you (see "Beware Passport Perils" on page 7, column 3). For this and other security-related reasons beyond the scope of this article, we simply recommend you avoid using any service that requires your personal information— including MSN Instant Messenger, .NET, the Microsoft Wallet, etc.

No Password Requirements. By default, Windows XP does not require passwords for login. We recommend users assign a password using the "User Accounts" control panel after their initial login. In fact, this is required for users who wish to log in on Windows servers.

Hardware Compatibility Issues. Windows XP requires a special piece of software called a "driver" to communicate with hardware devices like the video card, hard disk, and other computer components. Drivers made for Windows 2000 *might* work on Windows XP, but often will not. In addition, new operating systems almost always require additional memory and hard disk space and XP is no different.

The cost of upgrading these components in an *older* PC to accommodate the new version of Windows is generally not worth the cost, given that prices for brand-new PCs have come down. If you particularly want to run Windows XP, we recommend purchasing a new computer with that operating system pre-installed. This should avoid any hardware compatibility issues.

If you have a modern PC with fast processor and more than average RAM and disk space, then upgrading to XP may be a reasonable option. Should you decide to upgrade an existing PC, make sure you have important data backed up before you begin. You should also verify that drivers designed for XP exist for your video card and other components like your printer, scanner, or digital camera if you have them.

In short, if you're happy running an earlier version of Windows like 98, ME, or 2000, we don't recommend upgrading. If you need a new computer anyway, XP will likely be pre-installed in any PC you buy so you should not have any hardware compatibility problems.

Advanced Features, Some Increased Hazards

Features of XP Home Edition

After trying this edition out for ourselves, we noted the following improvements:

- **Start-up time** is slightly faster than older versions of Windows. XP also "wakes up" more quickly from suspension or hibernation.

- **Stability.** Microsoft claims that XP is more stable than prior versions of Windows, which should reduce crashes. Our experience has been that both XP and its predecessor, Windows 2000, are slightly more stable than Windows 98.

- **Security.** A basic Internet firewall, which rejects connection attempts that are "attacks" from external Internet connected computers, is included with Windows XP Home Edition.

- **Built-in basic CD-ROM burning facilities.** If your needs are simple (e.g., you just need to burn data), this can replace separate burning software. One caveat: this software doesn't work with all CD-R/W drives.

- **Improved handling of digital images and related devices.** For example, the new XP adds drag-and-drop support for some cameras that otherwise lack it.

- **Fast user switching.** Users lack passwords by default. Depending on your point of view, this can be a feature or a problem. For the average home user this is a convenience.

- **Power management enhancements for laptop users.**

- **Enhanced help facilities.** XP's enhanced Help and Support System is especially useful for those with Internet connections.

- **System Restore** (like Windows ME), and the ability to enter safe mode to correct problems (like Windows ME/2000/98 etc.) While this feature is not entirely new, it's a worthwhile inclusion.

- **Integrated 802.11 Wireless support.**

- **Better multitasking** (like Windows 2000).

Features of XP Pro Edition

In addition to all the features included with the home edition, Windows XP Pro also offers:

- **Multiple CPU (processor) support.**

- **NT/2000 server login, domain login, centralized administration.**

- **Remote control software.**

- **Offline folders and files, and roaming profiles.**

- **Encrypting file system.**

- **Access control, group policy.**

- **Better multilingual support.**

Campus users may require the professional version for several reasons, but most importantly to login to Windows-based servers.

References

Here are some additional references to help you evaluate Windows XP:

1. A good overview of the XP product can be found at **http://www.zdnet.com/products/stories/reviews/0,4161,2809517,00.html**
2. Cnet review "superguide" for Windows XP: **http://www.cnet.com/software/0-6688749.html**
3. Microsoft's XP site: **http://www.microsoft.com/windowsxp/default.asp**
4. Patches for vulnerabilities: **http://www.microsoft.com/security/**

   (The technet section linked from this site is generally also a good resource.)

News Flash: Serious Windows XP Security Hole Comes to Light

Grave Windows XP software glitches were discovered last month that pose unprecedented risk to consumers. These flaws, uncovered by security researchers with eEye Digital Security, Inc., allow hackers to surreptitiously steal or destroy a victim's data files across the Internet or implant malicious computer code in their computer—without requiring the victim to do anything other than connect to the Internet. *The problem also affects Windows 98 and ME systems on which UPnP (Universal Plug and Play) was installed.*

For a full description of the problem and a link to Microsoft's free solution, see Microsoft security Bulletin MS01-059 at **http://microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-059.asp**

Note: The FBI has recommended immediately disabling UPnP support for all versions of Windows. "UnPlug n' Pray," a free utility for uninstalling UPnP on any version of Windows, may be downloaded from **http://www.grc.com/UnPnP/UnPnP.htm**

SANS Institute, FBI Publish List of

Microsoft IIS leads list of compromised servers

Joyce Winslow
jwins@oregon.uoregon.edu

Expanding on their original list of Ten Most Critical Internet Security Vulnerabilities, the SANS Institute and the Federal Bureau of Investigation released a new "Top Twenty" list last October.

The new list, available at **http://www.sans.org/top20.htm**, is designed to heighten awareness of common threats to system security. It includes seven problems that affect all systems, six vulnerabilities specific to Microsoft servers, and seven flaws afflicting Unix (including Linux and Solaris). Although the flaws are not ranked, Microsoft IIS's problems are more widespread than others because these servers are the most widely used and they are very susceptible to "back door" incursions (see "What Vital Security Lessons Can We Learn from Code Red?" in the Fall 2001 issue of *Computing News*, **http://cc.uoregon.edu/cnews/fall2001/code_red.html**).

Fortunately, most of the major vulnerabilities can be disarmed as long as system administrators are vigilant and stay informed. The Top Twenty list is designed to help harried administrators immediately identify, and protect against, the most common and dangerous attacks by combining the knowledge of leading security experts from federal agencies, research institutions, universities, and security software vendors.

Below is a brief summary of the Top Twenty vulnerabilities. **(For complete details and suggested remedies, as well as a list of common vulnerable ports, see http://www.sans.org/top20.htm)**

General Problems (all systems)

1. Using the default installs of operating systems and applications. As convenient as these "quick install" software scripts or programs are, they create major security problems because users fail to realize what is actually installed. Extraneous services with their corresponding open ports, and unneeded sample programs or scripts offer easy avenues of attack that can go undetected indefinitely. Remove all unnecessary services and install security patches.

2. Allowing accounts with no passwords or weak passwords. Passwords that are easily guessed or bypassed, and accounts that require no password at all, are extremely vulnerable to attack. It's important to know what accounts are on your system, and check passwords for all of them—including passwords on systems like routers and Internet-connected digital printers, copiers, and printer controllers.

3. Not running backups, or doing incomplete backups. Regular, verifiable backups of mission-critical data are essential to being able to recover from an attack. Make sure your backup medium is as well protected as your server.

4. Keeping a large number of open ports. Keep only as many ports open as are necessary to keep your system functioning properly. Close all other ports, as they can provide possible attack venues for attackers.

5. Not filtering packets for correct incoming and outgoing addresses. Install a device that blocks decoy, or "spoofed" packets, and test it often. You must verify the legitimacy of packet addresses coming in and out of your network

6. Not keeping, or backing up, regular network logs on all key systems. Keeping close tabs on what's occurring on your network is essential. Without a network log, if you're victimized, you'll have little chance of discovering what the attackers did.

7. Running vulnerable CGI programs. Run the latest version of legitimate GGI programs, and always remove sample programs from production systems. You should also run a vulnerability scanning tool to check for holes in your site and apply patches for known vulnerabilities that can't be removed.

Windows Problems

1. Unicode vulnerability (NT 4.0 with IIS 4.0 and Win2K server with IIS 5.0). Microsoft's security checks can be bypassed if invalid Unicode character representations are used. For more information, see **http://www.wiretrip.net/rfp/p/doc.asp?id=57&face=2**

2. ISAPI extension buffer overflows (Microsoft IIS). To avoid buffer overflow attacks, watch out for programming errors when extending the capabilities of a IIS server and unmap any unneeded ISAPI extensions. Both the IIS Lockdown tool (available at **http://www.microsoft.com/technet/security/tools/locktool.asp**) and the URLScan filter (**http://www.microsoft.com/technet/security/URLScan.asp**)protect against this vulnerability.

3. IIS RDS (Remote Data Services) exploit on NT 4.0 systems. Malicious users can exploit programming flaws in IIS RDS to run remote commands with administrator privileges. For complete details, see **http://wiretrip.net/rfp/p/doc.asp?id=29&iface=2**

4. Unprotected Windows file sharing - NT and 2000. The Server Message Block (SMB) protocol that enables file sharing over networks can be exploited by hackers. Enabling file sharing on Windows machines makes them vulnerable to both information theft and viruses. See **http://www.microsoft.com/technet/security/tools/mpsa.asp**

5. Anonymous logon ("Null Session" connections) - NT 4.0 and Win2K. If anonymous users are allowed to retrieve

Top 20 Internet Security Vulnerabilities

information over the network or to connect without authentication, your system can be vulnerable to attack. If you're working in a domain environment, where Null sessions are required for the controllers to communicate, you can limit the information available to attackers, but you won't be able to stop all leakage. See "Top Twenty" section W5 at **http://www.sans.org/top20.htm** for full details on how to assess your vulnerability and protect your system.

6. Weak hashing in SAM (LAN Manager hash) - Windows NT and 2000. LAN Manager password hashes are created by default on NT and 2000 installations. Because LAN Manager uses a weaker encryption scheme than its more current Microsoft counterparts, its passwords can be quickly cracked. For a complete description of, and solutions for, the LAN Manager hash problem, see "Top Twenty" section W6 at **http://www.sans.org/top20.htm**

(Note that the remedies for this problem do not work if you have older systems, such as Windows 95, on your network. The safest option is to get rid of older systems altogether, although that may not always be feasible.)

UNIX Problems

1. Buffer overflows in RPC services. Remote procedure calls (RPCs), which allow programs on one computer to execute programs on another computer, are highly vulnerable to buffer overflow attacks. The program's poor error checking leaves the door open for attackers. You should turn these programs off, or at the very least, install the latest patches. See section U1. of the "Top Twenty" at **http://www.sans.org/top20.htm** for information on where to get the patches for Solaris, IBM AIX, SGI, Compaq (Digita)l UNIX, and Linux systems.

2. Sendmail vulnerabilities. Sendmail's widespread use on the Internet makes it a prime target of attackers. Most versions of UNIX and Linux are potentially affected. To protect your system, upgrade to the latest version of sendmail and/or apply the patches. For complete details on sendmail's vulnerabilities and their remedies, see **http://www.cert.org/advisories/CA-1997-05.html**

3. BIND (Berkeley Internet Name Domain) weaknesses - potentially affects most versions of UNIX and Linux. This widely used implementation of Domain Name Service (DNS), which locates systems on the Internet without having to know specific IP addresses, is another popular target for attack. In the worst-case scenario, BIND can be exploited to allow intruders to erase system logs and install tools to gain root access. Outdated version of BIND also include buffer overflow vulnerabilities.

For more details on BIND problems and a list of precautions for systems administrators, see section U3 of the "Top Twenty" list at **http://www.sans.org/top20.htm**

4. *r* Commands (affects most variants of UNIX, including Linux). *r* commands, which enable system administrators to access a remote system without a password, can be exploited by attackers with ruinous results. If an attacker gains control of any machine with a trusted IP address, he or she can then use *r* commands to overtake all other machines that trust the hacked machine's address. The best defense is not to allow IP-based trust relationships, and not to use *r* commands. Never allow the ".rhosts" file in the root account, and use the UNIX "find" command regularly to look for any ".rhosts" files that may have been created on other user accounts.

5. LPD (remote printer protocol daemon) - affects most variants of Linux, as well as Solaris 2.6, 7, and 8 for SPARC and x86. The code that transfers print jobs from one machine to another has an error that creates a buffer overflow vulnerability. If the daemon is given too many jobs within a short time, it will either crash or run arbitrary code with elevated privileges.

For Solaris patch information, see Sun's Security Bulletin #206 at **http://sunsolve.sun.com/security** The CERT Advisory for this topic is available from
http://www.cert.org/advisories/CA-2001-15.html

A patch for Linux can be found at
http://redhat.com/support/errata/RHSA-2001-077.html

6. Sadmind and mountd - affects multiple versions of UNIX. These commands are both vulnerable to buffer overflow attacks that allow intruders to gain control with root access. For additional information, see
http://www.cert.org/advisories/CA-1999-16.html
http://www.cert.org/advisories/CA-1998-12.html

7. Default SNMP (Simple Network Management Protocol) strings - UNIX. A weak authentication mechanism makes this protocol, which is widely used by network administrators to monitor and administer all types of network-connected devices, easily subverted by attackers. Attackers can use this vulnerability in SNMP to reconfigure or shut down devices remotely. (Note that SNMP is also used in Windows administration, but it has not been a major problem on Windows systems.)

The best protection is to disable SNMP if you don't require it. Otherwise, you should beef up your authentication requirements as described in "Top Twenty" section U7 at **http://www.sans.org/top20.htm**

LAST YEAR IN REVIEW:
See an 84-page summary of all security holes and viruses compiled by the National Infrastructure Protection Center at

http://www.nipc.gov/cybernotes/2001/cyberissue2001-26.pdf

Beware of '4-1-9' or 'Nigerian Advance Fee Fraud' Scams

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

We have been seeing a growing number of UO users receive so-called "4-1-9" or "Nigerian Advance Fee Fraud" solicitations by email.

These scams often promise to share millions of dollars from "over-invoiced contracts" or some other financial source, typically Nigerian, if only some money for processing fees (or for taxes, attorneys costs, transaction fees, etc.) can be covered—temporarily, of course—by you.

Do not get taken in by these scams. If a deal seems too good to be true, it is—particularly in cases like these. There are no millions of dollars waiting for you; you are simply the target of a con artist.

For more information about "4-1-9" or "Nigerian Advance Fee Fraud" see the following websites:

http://www.treas.gov/usss/index.htm?alert419.htm&1

http://www.state.gov/www/regions/africa/naffpub.pdf

http://home.rica.net/alphae/419coal/

http://www.salon.com/people/feature/2001/08/07/419scams/index.html

Virus Alerts: *VBS.Haptime, W32.Badtrans.B@mm* Seen on Campus

Outlook users need to be especially careful

Two worm viruses, Haptime and W32.Bdtrans.B@mm, have been making the rounds on campus over the last few months. Fortunately, you can protect yourself fairly easily by installing the requisite patches and keeping your antivirus software up to date. It's also good general practice not to open email attachments from an unknown, suspicious or untrustworthy source. We also continue to recommend that users *not* run Outlook or Outlook Express.

VBS.Haptime. Haptime, recently downgraded by Symantec from a threat level of Category 4 to Category 3, should nonetheless be taken seriously. A Visual Basic Script (VBS) worm, Haptime infects .htm, .html, .vbs, .asp, and .htt files, using Outlook Express as the mechanism of reproduction. Users are infected through an email attachment named "Untitled.htm," and spread the virus via Outlook Express. Haptime infections usually become apparent when Windows complains that the Active Desktop is corrupt and needs to be restored. Symantec's Haptime fix is available at
http://securityresponse.symantec.com/avcenter/venc/data/vbs.haptime.fix.html

W32.Badtrans.B@mm. Exploiting a previously patched hole in Outlook's email program, this MAPI worm emails itself out as one of several different file names, including HUMOR, DOCS, S3MSONG, ME_NUDE, CARD, SEARCHURL, YOU_ARE_FAT!, NEWS_DOC, IMAGES, and PICS. It then installs malicious code on infected computers to usurp private information such as usernames and passwords. The virus is activated simply by clicking to open and read an infected email message in Microsoft Outlook—no need to even open an attachment. Once Badtrans.B is active on a system, it emails itself to addresses contained in email address books, web cache, and the "My Documents" folder.

To remove the virus (excluding its variants), you can use Symantec's W32.Badtrans.B@mm Removal Tool at
http://securityresponse.symantec.com/avcenter/venc/data/w32.badtrans.b@mm.removal.tool.html

For more information on Badtrans.B, see Microsoft's Security Bulletin MS01-020 at
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-020.asp

Also see CERT's Incident Note at
http://www.cert.org/incident_notes/IN-2001-14.html

Microsoft Launches New STPP Security Program

Last fall, Microsoft inaugurated a new program of expanded free technical support and security packages in order to help improve the security of all Microsoft products. To contact the new virus-related tech support service, call **(866) 727-2338**. For more information about STPP, or to download the Security Tool Kit, go to **http://www.microsoft.com/security/**

Watch Out for Microsoft Vulnerabilities

Guard against serious security loopholes in IE, Excel, PowerPoint, Outlook, and Windows Media Player

Joyce Winslow
jwins@oregon.uoregon.edu

In recent months, a number of serious security holes have been reported in several widely used Microsoft products. A cookie exploit and Active Scripting bug in Internet Explorer 5.5 and 6, a macro protection hole in Excel and PowerPoint, continuing Nimda virus vulnerabilities in Outlook, and a bug in Windows Media Player, are all significant liabilities. Below we've summarized the specific problems and their remedies.

IE Liabilities

Cookie exploit. This high-risk vulnerability in Internet Explorer 5.5 and 6 allows attackers to access potentially sensitive user information that's stored by website "cookies," the small text files recorded in your hard drive that collect data such as the IP address of your machine, your operating system, the browser you're using, and other information. These data allow advertisers to "remember" you and the sites you visit, targeting you for advertising.

In response to this problem, Microsoft released a comprehensive patch that is intended to address all known IE 5.5 and 6 vulnerabilities. For complete details on the cookie vulnerability and the patch, see

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-055.asp

ActiveX security hole. This new vulnerability, which was reported on December 11, led security researcher Georgi Guninski to recommend not using IE—or at the very least, to disable Active Scripting.

This bug could allow a hacker to execute malicious code on systems running IE 5.5 and 6.0 by inserting a specially crafted script into a web page or email. Microsoft issued a patch for a similar bug exposed in November, but the patch itself seems to have created the new problem.

Details about the bug are available at
http://www.theregister.co.uk/content/55/23557.html
and in the article "MS Releases Mother of All IE Security Patches" at
http://www.theregister.co.uk/content/55/23410.html

Excel and Powerpoint Security Hole

This vulnerability gives attackers the opportunity to take control of a victim's computer by creating files that bypass macro security and allow macros to execute automatically without user permission. When the victim opens one of these PowerPoint or Excel files, malicious code can then operate in the background undetected.

The patch for this problem is available at
http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/bulletin/MS01-050.asp

Outlook Express 6.0 Vulnerabilities

An Outlook Express feature that allows it to automatically execute scripted code even on plain text messages, as well as its well-known problem of allowing concealed attachments, make this software extremely vulnerable to invasion by malicious code. For details, see

http://www.securiteam.com/windowsntfocus/5HP0D1P5FC.html

To evade these risks, make sure you set your browser as follows:

Internet Explorer: Under the Edit menu, choose Preferences and go to "Security Zones." Select "Zone: Restricted Sites zone." Choose "Custom" level security and make sure all the ActiveX options are disabled.

Outlook Express: Go to Options->Security (or "Virus Protection"). Make sure you're using the Restricted Sites security settings.

Outlook: go to Tools ->Options->Security->Secure Content and select the Restricted Sites settings.

Windows Media Player. Late last fall, a vulnerability was discovered in the code of Windows Media Player 6.4 used to play Advanced Streaming Format (ASF) content. This security hole can allow a malicious attacker to take control of a victim's PC via a buffer overrun.

With the exception of those who have Windows XP, Microsoft is urging users of all versions of Windows Media Player (6.4 through 7.1) to download the patch. (Note: Windows XP users are being asked to download an updated version of Media Player instead of using the patch.)

Additional information and links to the software updates are available at **http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-056.asp**

Vipul's Razor Aids Spam Detection, Filtering

System administrators and web developers may want to investigate a distributed, collaborative, spam detection and filtering network known as Vipul's Razor. The Razor network detects and catalogs spammer addresses so they can be blocked out by the rest of the filtering agents on the network. For more details about Vipul's Razor, see
http://razor.sourceforge.net/

Who's Who at the

Meet some members of our staff

Joyce Winslow
jwins@oregon.uoregon.edu

Connie French
Computer Services Assistant
Computing Facilities

Connie French's office in 151 McKenzie is filled with evidence of world travel. Dolls from the Ukraine, an Alaskan totem, Japanese chopsticks, a Hawaiian paperweight, postcards from Egypt…these are only a few of the artifacts that UO faculty and staff have given her over the years in appreciation for her help in setting up and managing their university computing accounts.

Connie's been overseeing UO computing accounts at the Computing Center for almost 15 years now, but her history with our department began much earlier, in 1971, when she worked part-time as a data entry operator while attending school.

With her extensive family ties in Eugene, it seemed a given that Connie would settle down in her home town and follow her career path here. But after a few years, Connie and her husband Don relocated to Sacramento, California, where Connie found work in the production control division of the California Farm Bureau.

After eight years in the dry central valley of California, Connie and Don began to miss the lush green of the Willamette Valley and decided to return home to Eugene. Connie promptly picked up where she'd left off at the Computing Center, adding reception duties to her work in data entry. Over time, Connie's responsibilities grew to include providing backup scanning, scheduling the use of instructional computing labs, and handling UO computing accounts.

In a relatively short time, the number of UO computing accounts grew from 3,000 to 35,000, and overseeing computing accounts—setting up the new, retiring the old, troubleshooting problems, and tracking account eligibility—began to consume most of Connie's day. UO computing accounts are still her primary responsibility, but Connie also fills in as a BANNER clerk and serves as a backup receptionist for the Computing Center's Electronics Shop, which services computing hardware and peripherals on campus.

In her spare time, Connie is fulfilling one of her longtime goals by pursuing a degree in criminal justice. A devoted cat-lover, Connie also enjoys pampering her two Manx kitties, Paco and Mija, and she and Don are frequent visitors at the South Coast Animal Park in Bandon, where they're allowed to handle baby Bengals and panthers.

Robert Gillespie
Systems Analyst, Administrative Services

On most Fridays, rain or shine, Robert Gillespie sports an "Aloha Friday" shirt. Although he's been to the Hawaiian Islands only three times, this Eugene native immediately took to the islanders' version of "casual Fridays" and likes to carry on the tradition here.

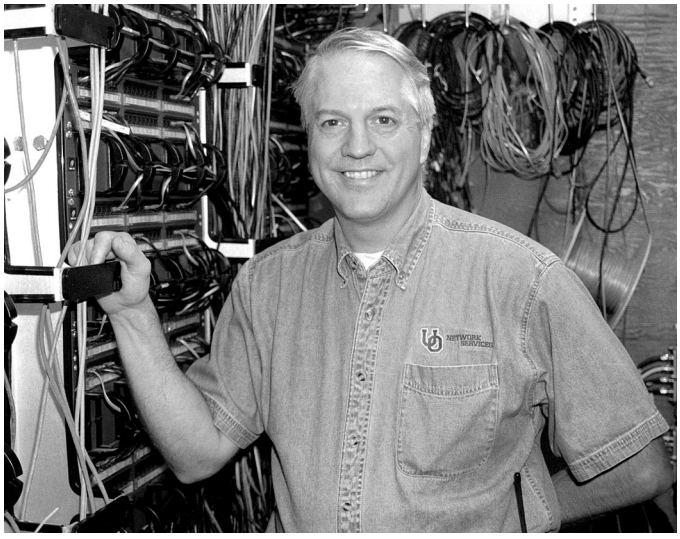
Robert has a long-standing interest in Asian and Polynesian cultures, as well as folklore and myths of all types. A person who likes to pursue his interests in depth, Robert has taken several classes in the subject—most recently, an American folklore class at the UO. Robert is also a fan of

science fiction, and since the age of 15 has devoted much of his spare time to writing novels and short stories—all as yet unpublished—in that genre.

Robert's programming career at the Computing Center began in 1995. Prior to that, he studied computer science at the UO and OSU and for 10 years was OSU College of Veterinary Medicine's all-around computer "go-to" guy, setting up its network, performing system administration, and writing scientific and administrative programs. For three years after leaving OSU, he worked for the Oregon University System, traveling throughout the state as a technical consultant and assisting institutions that were converting to the BANNER Financial Information System.

Since coming to the UO six years ago, Robert has worked as a systems analyst for the Administrative Services group supporting both the Office of Admissions and the Registrar's Office. He works primarily with BANNER and DuckWeb, supporting the Banner General and Student modules and their infrastructure. Robert designed the Interactive Transfer Catalog, a dynamic HTML / Javascript application that allows students to determine transfer equivalencies for their UO coursework.

Outside the office, Robert is busy being a dad to Margaret (8) and Elizabeth (10). He still writes whenever he finds the time, and until a knee injury sidelined him four years ago, he was a faithful practitioner of the Chinese martial art Wing Chun.



Don Williams
Network Technician, Network Services

When Don Williams joined the Computing Center as a network technician in the fall of 1976, teletypes and punch cards were still the order of the day. Over the years, Don has kept pace with the evolution of electronic communications from wire to fiber optics, and he has seen the Computing Center's Network Services organization grow from a tiny pioneering team of two to a staff of nine—including three technicians, five network engineers, and a director.

Don began his electronics training in the US Navy, where he maintained teletypes and keypunch machines and worked on encryption and networking equipment. Near the end of his tour of duty in 1972, he met his wife Diane while stationed near Napa, California. The couple soon married and moved back to Don's native state of Oregon so Don could resume his interrupted college career at OSU, where he had already put in two years as a chemistry major.

With four years of electronics experience already under his belt, Don changed his academic focus to computer science and eventually landed a job as instrument technician at OSU's computing center. For the next two years, Don traveled the I-5 corridor, servicing the teletype and communications gear at Portland State and Southern Oregon College as well as maintaining OSU's equipment.

In 1976, Don was offered a similar position at the UO Computing Center, and he and his family (which now included baby David) moved to the country just south of Eugene. A few years later, in 1978, David's baby brother Jon was born.

In addition to his troubleshooting and maintenance duties, Don has also assisted with network evolution, wiring every building on campus and building a patch panel of more than 50 serial connections. Later, he helped expand the campus serial communications network, and together with Dale Smith (now Director of Network Services), he was a pioneer in helping install the UO's award-winning campus network, UOnet.

An avid chef, Don enjoys experimenting with international cuisine when time permits. He and Diane share a fascination for European history and hope to devote more time to travel in the future. Top on their list is Scotland, where Diane has relatives, followed by Provence, Spain, Italy, and Greece.

Mathematica for Mac OS X is Here

Wolfram Research has released a version of Mathematica for Mac OS X that's optimized to provide quicker calculations and more stability under Apple's latest operating system. For instructions on how to install this new version, go to
http://darkwing.uoregon.edu/~hak/mathematica/

If you have further questions about the product, contact Hans Kuhn (*hak@oregon.uoregon.edu*).

FBI's 'Magic Lantern' Software Eavesdrops on High-Tech Communications

The FBI is updating its surveillance technology to keep pace with the digital age. As part of a broad project called "Cyber Knight," the agency is developing powerful Internet eavesdropping software that can record every keystroke on a person's computer.

This new surveillance tool, known as "Magic Lantern," is being designed to thwart encryption software by capturing the keystrokes or mouseclicks a person might use to deliberately scramble messages or computer files. Magic Lantern exploits some of the same weaknesses in popular commercial software that allow hackers to break into computers, and could be used with a court order against suspected terrorists or criminals.

Such powerful surveillance tools always raise constitutional and privacy issues, and there is still some debate about the legality of using Magic Lantern without a search warrant. Because the software can be covertly installed over the Internet without the need for actual physical entry into a person's home or office, some argue that a search warrant should not be required.

The full text of an Associated Press article about Magic Lantern and its implications is available online to *Washington Post* archive subscribers. To locate it, go to

http://www.washingtonpost.com/wp-adv/archives/

and search for "Magic Lantern." The article was first published on November 22, 2001.

Researchers Uncover Serious AOL Instant Messenger Security Problem

Latest glitch highlights risk of running popular recreational applications indiscriminately

An international team of nonprofit researchers known as "w00w00" recently reported a serious security hole in AOL's popular Instant Messenger program (AIM), which is used by millions of users worldwide to communicate via short, real-time messages. The problem—which is exclusive to Windows systems—affected AIM's newest versions, as well as many earlier iterations of the program.

The vulnerability allowed hackers to send a stream of junk messages to the program, overwhelming the software and completely hijacking the victim's computer. Once compromised, the machine could be subject to any mischief a hacker devised, including deleting files and spreading computer viruses.

AOL took immediate steps to fix the problem before users were affected. However, serious security loopholes like this one are being discovered every day in popular commercial software products used by hundreds of millions of people, and they have the potential to create widespread damage.

We strongly recommend you avoid installing network applications not included on the Duckware CD-ROM, which is distributed at no charge each year to UO faculty, staff, and students. If you do choose to install other applications, be extremely discriminating and stay up-to-date on vendor fixes and antiviral software.

For a complete description of AIM's security problem, see the w00w00 information page at **http://www.w00w00.org/advisories/aim.html**

If you do not yet have your copy of Duckware, go to Microcomputer Services (151 McKenzie Hall) or the Documents Room library (175 McKenzie) and request one.

Defense Department Weighs in on Spectrum Debate

Early in the new year, Secretary of Defense Donald Rumsfeld appointed a new deputy to oversee frequency spectrum issues and communications policy. The new deputy is charged with helping the Department of Defense build a global secure wideband network that ensures unimpeded communications access to the U.S. military.

The Pentagon has been at odds with Congress and the wireless industry over control of its frequency spectrum, which thus far has remained an exclusive preserve of the military.

For more details on the spectrum debate, see the EETIMES.com story, "DOD appoints spectrum czar," at **http://www.eetimes.com/story/OEG20020104S0076**

Need to Check for Multicast Connectivity? Try 'Multicast Tester'

If you're a member of the UO faculty or staff, or a UO student with a networked Windows PC, you know that broadcast-quality IP multicast video via IP/TV is available on your desktop. But if you're trying to help a non-UO colleague check for multicast connectivity, Multicast Technologies has the answer.

By listening for traffic from the NLANR Multicast Beacon project, the Multicast Tester can determine whether or not a site has IP multicast connectivity.

To use the tester, go to

http://www.multicasttech.com/mt/

and follow the instructions.

The site also provides information on how to incorporate this tool into your website.

For more information about IP/TV at the UO, see **http://cc.uoregon.edu/iptv/** To see a current schedule of multicast videos, as well as links to more information about multicast applications, go to **http://videolab.uoregon.edu/**

Intel Donates Nearly $720,000 Worth of Networking Equipment to UO

At the end of 2001, Intel Corporation donated networking equipment to the UO valued at nearly $720,000, including eight Intel NetStructure 7180 e-Commerce Directors, seven NetStructure 7370 Application Shapers, and fourteen NetStructure 7340 Traffic Shapers like the ones pictured on the cover of this issue. These devices will greatly enhance the university's ability to utilize its network resources fully and efficiently, resulting in improved service to campus users.

For more details on the capabilities of the new equipment , see "Understanding the Basics of Traffic Shaping" and "How Load Director/SSL Accelerator Boxes Work" on pp. 20-21.

Although President Frohnmayer has already personally thanked Intel for these donations, the Computing Center would like to take this additional opportunity to publicly express its thanks to Intel for its continued generosity to the University of Oregon. We are truly fortunate to have such a cutting-edge (and generous!) company in Oregon.

Web Designers: Watch Out for Vulnerability in Flash Animations

Based on the recent success of an infectious program dubbed SWF/LFM-926, antivirus companies warned that future Macromedia Flash animations may harbor computer viruses. SWF/LFM-926 infects the Flash files on a PC whenever an affected movie is played.

While SWF/LFM-926 is not currently considered very serious, future exploits of the Flash vulnerability could be more malicious. As we go to press, Macromedia is releasing a fix to disable the file association between Flash files and the local Flash player. The company also plans to eliminate the vulnerability altogether in the next version of Flash.

On January 14, Oregon.gov replaced Oregon On-Line as the state's main government portal. State agencies should change any *top-level* links or references to Oregon On-Line (**www.state.or.us**) on their websites to **www.oregon.gov** (Note that the new Oregon site has been completely reorganized; check carefully before changing the addresses of any lower-level links, as most pages from the old site will not be on the new site.)

The official graphic link may be downloaded from **http://egov.das.state.or.us/Communications_files/linkdown.htm**

Understanding The Basics of Traffic Shaping

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

Intel's recent generous donation of 21 traffic shaping boxes potentially gives the University of Oregon great flexibility in managing its network traffic.

One major advantage of these boxes is that they can be used in more than one way. In passive mode, they can analyze and classify the traffic that's flowing on a subnet (this can be useful in such activities as doing network planning or resolving performance issues, for example). But when used in active mode, the boxes can also "shape" or control the traffic that flows over the network.

Without intentional traffic shaping, network traffic will flow subject only to natural limitations , or "choke points." Those choke points can occur at a very low level (e.g., at the TCP/IP protocol level), in the way an application happens to be programmed, in the host system on which an application may be running, or in the network itself. If you are dialing in, for example, your traffic will be choked by the 40 to 50Kbps of effective throughput your modem may deliver.

In the case of a directly connected system on campus, most often the only binding constraint will be the university's wide area (Internet) bandwidth, which we all collectively share. This type of bandwidth is in high demand on campus, but because it's expensive to purchase and budgets are tight, the university must manage its limited bandwidth wisely.

Ways of Managing Bandwidth

When traffic shaping boxes are used, wide area (Internet) bandwidth can be actively managed to limit traffic in several different ways:

1. Per-application rules. Traffic shapers can identify and categorize specific types of network traffic, constraining each particular category of traffic to use no more than a specified amount of bandwidth. For example, you might hypothetically have a rule that limits aggregate FTP traffic to no more than 6 megabits per second and a another rule that limits total streaming audio traffic to no more than 3 Mbps, etc.

Traffic shapers can categorize traffic based on macroscopic characteristics, such as the traffic's protocol (IP, IPX, AppleTalk, DECNet, etc.), the ports an application is known to use (for example, Kazaa typically runs on port 1214), or on the basis of connections to a particular well-known host (such as a central game server), etc.

Traffic can also be categorized based of the *content* of the flow regardless of the flow's macroscopic characteristics. For example, most traffic shapers can easily identify and automatically categorize web traffic based on the negotiations that take place between a web server and a web browser when a page is requested, regardless of whether the web server is running on port 80 (the default) or some other nonstandard port.

2. Per-user rules. Traffic shapers can set per-user traffic limits to ensure that network traffic is shared fairly among all users. For instance, you might decide to use a per-user rule that limits traffic to or from each user to no more than 256Kbps (giving them DSL-like service). When traffic is limited in that way, a user can still access whatever he or she wants, but the flows are "smoothed out" to a specified level rather than attempting to use all or much of the total available network capacity campuswide.

Traffic limits can be either "hard" or "burstable." As you might expect, a hard limit is a fixed ceiling that can't be exceeded. Burstable limits, on the other hand, allow traffic to exceed the base threshold value (at least up to a specified "burst limit") as long as capacity remains available and there's no higher priority application preemptively claiming that capacity.

3. Priority management. In addition to setting hard or burstable traffic limits on a per-application or per-user basis, traffic shaping devices can also be used to define the relative importance, or priority, of different types of traffic. For example, in an academic network where teaching and research are most important, recreational uses of the network (such as network games or peer-to-peer file sharing application traffic) can be allowed bandwidth only when higher priority applications don't need it.

Some traffic shaping tasks can be done directly on a regular Cisco or Juniper router, just as a router can also be used to do some firewall-like packet filtering tasks. However, specialized traffic shapers, like any specialized devices, can be optimized to specifically and efficiently handle their unique responsibilities. Specialized devices also typically have a "bigger bag of tricks" to draw from when dealing with problems in their special area of expertise. Doing traffic shaping on a dedicated traffic shaping box also avoids loading up routers with other tasks, leaving the router free to focus on doing its job of routing packets as fast as it can.

For more information about bandwidth management strategies, including case studies and technical briefs, see **http://www.intel.com/network/idc/products/bandwidth_management.htm**

How Load Director/SSL Accelerator Boxes Work

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

The eight 7180 e-Commerce Director boxes that Intel recently donated to the university can perform a number of vital networking tasks. Below we've described two of the most important: SSL acceleration and load balancing.

SSL Acceleration

When you connect to a secure website like DuckWeb, or to one of the UO's secure web email servers, or to an online shopping website such as amazon.com, the connection between that site and your web browser is encrypted using the SSL protocol (symbolized by the little "lock" you'll see at the bottom corner of your browser).

Using SSL provides three big advantages: "privacy," "integrity," and "authenticity." SSL encryption ensures your privacy by preventing someone from "eavesdropping" on your network traffic. SSL encryption also provides traffic "integrity" by ensuring your transmissions cannot be altered en route. If you trust the ID verification procedures of the party who issued the SSL certificate for a given server, you also have assurance that you're connecting to the party you believe you're connecting to. This is usually referred to as providing "authenticity."

Given the benefits of SSL security, you may wonder why all websites don't use SSL for all traffic. The answer is simple: there is substantial computational overhead associated with encrypting traffic using SSL (or SSH, or any other nontrivial encryption scheme), so encryption is usually used only when particularly sensitive information is being transmitted, such as a credit card number, a password, a student's grade information, etc.

SSL accelerators were created to "offload" computationally demanding encryption calculations from the web server, using specially tailored hardware encryption chips in a separate box that sits in front of the server. (For example, the Intel 7180 boxes we received can handle over 600 SSL connections per second—or over 2,000,000 an hour.) Because the SSL accelerator handles all the encryption-related overhead for those connections, the main web server can focus on doing its primary job, delivering web pages. That usually translates to better performance (less latency) or higher web server throughput.

Load Direction

The other task an Intel 7180 can perform is what's normally referred to as "load direction" or "intelligent load balancing." To understand how this balancing function works, you need to know that there are two fundamental approaches to scaling a system up to handle a large number of users. You can either build a single large monolithic system, typically with lots of memory and many processors—or you can run a bunch of smaller systems, making them act as if they were all one system and somehow dividing up the traffic load between those boxes. The Google search engine is a good example of this. Google is actually a cluster of over 10,000 PCs running Linux (see **http://www.google.com/press/highlights.html**), all of which appear to the user to be a single unified system.

Making numerous systems act as if they were all one system and dividing the load between them are the tasks usually handled by a load director. In its simplest form, a load director sits in front of two or more identical back-end web servers and hands connections off to one or the other in round-robin fashion. This is very similar to what can be easily done via DNS round-robin aliases. However, unlike DNS round-robin aliasing, load directors can also employ other rules, such as sending a connection to whichever server is least busy, or ignoring a server which is temporarily down, thereby improving performance and effectively eliminating site downtime.

Load directors can also be used to intelligently route object requests based on the *type* of content being requested. For example, a 7180 can reroute requests for HTML pages to one server, requests for images to another web server, and requests for cgi-bin pages to a third server. Load directors can also be used to do a variety of network address translation tricks. For instance, by default, when a load balancer is interposed between users and a back-end farm of multiple web servers, all the traffic will appear to "come from" the load balancer, both in terms of what Internet users see and in terms of what each of the multiple web servers sitting behind the load director responds to—the 7180 mediates all content delivery in that scenario.

The 7180 does have the ability to do something called "Source Address Preservation," however, which allows the farm of web servers to see the *true* address of the user requesting a web page, rather than just seeing all requests (apparently) coming only from the 7180's address. This is convenient if you want to do log analysis on the individual web servers (rather than on the load director), for example, or if you want to do "out of path return," allowing the back- end web servers to bypass the 7180 and talk directly to the user when sending traffic back to that user's web browser.

Summary

This overview provides just a glimpse of the many functions these e-Commerce Director boxes can perform. You'll find more information about the role of e-Commerce Directors in network management at

http://www.intel.com/network/idc/products/director_7180.htm

SAS 8.2 Now Available on VMScluster

If you need to convert your old v.6 datasets in order to read them in the new version, follow these tips...

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

At the end of fall term, SAS 8.2 was installed on Oregon.

For most users, upgrading to the new version should be easy. However, if you're among those who need to explicitly convert their older SAS version 6 datasets in order to read them in 8.2, the task is a bit more complex.

For example, suppose you have two SAS version 6 permanent datasets called **datafile1** and **datafile2**. To convert those datasets from version 6 to version 8.2, you'll need to follow the steps outlined below:

1. Because both versions shouldn't be stored in the same directory, you'll need to create an OpenVMS directory to temporarily hold the old format datasets:

```
$ create/dir [.old]
```

2. Move datafile1.* and datafile2.* into that directory by typing:

```
$  rename datafile1.*[.old]
$  rename datafile2.* [.old]
```

3. Using EVE or EDT, create a file called **convert.sas** containing the lines:

```
libname mystuff base '[]';
libname oldstuff v6 '[.old]';

proc copy in=oldstuff out=mystuff;
  select datafile1 datafile2;
run;
```

4. Run the conversion job by typing:

```
$ sas82 convert.sas
```

5. Using EVE or EDT, check convert.log to make sure the job ran properly.

6. At a later point, *after* you have verified that your old data sets have been correctly converted to version 8.2 format, you can remove the old format data sets and the temporary directory you created to hold them:

```
$ set def [.old]
  $ del datafile1.*.*,datafile2.*.*
  $ set def [-]
  $ set prot=o:RWED old.dir
  $ del old.dir.*
```

For a summary of new SAS 8.2 features, see **http://www.sas.com/products/sassystem/release82/features.html**

You'll find complete SAS documentation for the OpenVMS environment at **http://sas.uoregon.edu/sashtml/vms/genid-2.htm**

If you have further questions about using SAS 8.2 on Oregon, please send an email message to Joe St Sauver at *joe@oregon.uoregon.edu*

Take a Look at the 'R Project': an Integrated Tool for Data Analysis

Free software provides flexible language and environment for statistical computing and graphics

Programmers looking for an extensible tool for statistical analysis and graphic techniques will want to investigate "R," a free product similar to the S language.

R is a computer language that allows users to add additional functionality by defining new functions, and link C, C++, and Fortran code for intensive computational tasks.

With R, programmers can produce well-designed publication-quality plots, including mathematical symbols and formulae where needed, while retaining full control over the design. Examples of R screenshots and graphics, including three-dimensional plots, are displayed at **http://www.r-project.org/** under "Screenshots."

For more information about R, go to the R Project site at **http://www.r-project.org/** The site offers a general overview of the project, as well as downloads, FAQs and manuals, bug tracking, and a developer page.

WINTER WORKSHOPS

The Library and Computing Center are committed to making sure you have opportunities to build your technology skills. Toward that end, we provide a wide range of computer and Internet training, from novice to advanced skill levels. 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.** You *must* meet the workshop prerequisites as stated in the description.

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**).

THE SPRING WORKSHOP SCHEDULE WILL BE AVAILABLE IN LATE MARCH

Workshop	Day/Date	Time	Location	Presenter

This schedule is subject to change. See *http://libweb.uoregon.edu/it/* for course outlines/materials and the most current information.

Web Publishing, Multimedia ✔Prerequisites

Web Publishing I - ★✔*Prerequisites:* Familiarity with a graphical web browser like Netscape or Internet Explorer and an account on Darkwing or Gladstone (not Oregon!); you must know your username and password

Thu Jan 24	10 - 11:50am	144 Knight Library	Frantz
Mon Jan 28	2 - 3:50pm	144 Knight Library	Michel
Tue Feb 5	2 - 3:50pm	144 Knight Library	Nicholson

Web Publishing II - ★✔*Prerequisites:* Web Publishing I or equivalent knowledge and skills, and a web page you've created

Thu Jan 31	10 - 11:50am	144 Knight Library	Nesselroad
Mon Feb 4	2 - 3:50pm	144 Knight Library	Bell

Web Publishing III -★ ✔ *Prerequisites:* Web Publishing II or equivalent knowledge and skills

Thu Feb 7	10 - 11:50am	144 Knight Library	Bell

Dreamweaver I ✔*Prerequisite:* Web Publishing I & II or equivalent knowledge and skills

Thu Feb 14	10 - 11:50am	144 Knight Library	Paynter

Communications and Research Software ✔Prerequisites

EndNote/ProCite Use these programs to organize and retrieve your citations and format your footnotes and bibliographies

Mon Feb 4	3- 4:20pm	235 Knight Library	Lenn
Tues Feb 5	3 - 4:20pm	235 Knight Library	Lenn

Linking Directly to Full-text Articles in Library Databases ✔*Prerequisite:* Basic knowledge of web page creation preferred

Thu Feb 14	1 - 2:50pm	144 Knight Library	Michel

PowerPoint Basics (Applicable to both Windows and Macintosh)

Tues Jan 29	3 - 4:50pm	267B Knight Library	Heerema

More PowerPoint ✔*Prerequisite:* PowerPoint Basics or equivalent knowledge and skills

Tues Feb 26	3 - 4:50pm	267B Knight Library	Heerema

Net a Job: Use the Web! ✔*Prerequisite:* Familiarity with a graphical web browser

Wed Mar 6	3 - 4:20pm	144 Knight Library	Haynes

PsycINFO ✔*Prerequisite:* Familiarity with a graphical web browser

Thu Jan 17	7 - 7:50pm	144 Knight Library	Benedicto
Thu Jan 24	3:30 - 4:20pm	144 Knight Library	Benedicto
Tue Jan 29	7 - 7:50pm	144 Knight Library	Benedicto

Managing a Majordomo List I ✔*Prerequisite:* List administrator for a majordomo list, an account Darkwing or Gladstone (not Oregon!); you must know your username and password

Thu Jan 17	3 - 3:50pm	144 Knight Library	Lynch

Managing a Majordomo List II ✔*Prerequisite:* Managing a Majordomo List I

Thu Jan 31	3 - 3:50pm	144 Knight Library	Lynch

Using MhonARC to Create a Web Archive for a Majordomo List ✔*Prerequisite:* Managing a Majordomo List I

Thu Jan 24	3 - 3:50pm	144 Knight Library	Lynch

★ 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
(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@oregon.uoregon.edu
http://micro.uoregon.edu/

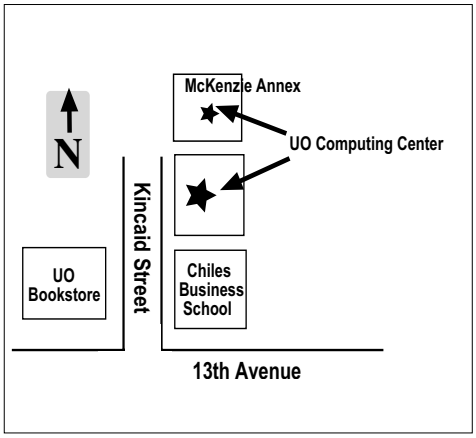
Documents Room Library
(175 McKenzie Hall)
346-4406
http://darkwing.uoregon.edu/~docsrm

Large Systems Consulting
(Rooms 225-239 Computing Center)

- VMS, UNIX (Gladstone, Darkwing, Oregon)
- email, multimedia delivery
- scientific and cgi programming
- web page development
- statistics

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

http://cc.uoregon.edu/unixvmsconsulting.html



Electronics Shop (151 McKenzie Hall)
For computer hardware repair, installation, and upgrade services, call **346-3548** or write *hardwarehelp@oregon.uoregon.edu*
Also see ***http://cc.uoregon.edu/e_shop.html***

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

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

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

Computing Center Hours
Monday - Friday 7:30 am - 5:00 pm

McKenzie Building Hours*

Monday - Thursday	7:30 am - 11:30 pm
Friday	7:30 am - 7:30 pm
Saturday	9 am - 9:30 pm
Sunday	9 am - 8:30 pm

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

COMPUTING NEWS
UO COMPUTING CENTER
1212 UNIVERSITY OF OREGON
EUGENE, OR 97403-1212