University of Oregon

COMPUTING NEWS

SPRING 2000

IN THIS ISSUE...

New Celeron 366MHz processors are available for UO computing labs and departments at no charge! See "Intel Donates Celeron Processors" on page 3.

BANNER 4.0 Upgrade Reminder

No more character-mode access after August 12, 2000

Jim Bohle
jbohle@oregon.uoregon.edu

This is a reminder that BANNER 4.0 will be installed during the Labor Day weekend this year (September 2-4, 2000). With BANNER 4.0, the current character-mode access will no longer be available, and all BANNER applications will require you to use Graphical User Interface (GUI).

To ease the transition to BANNER 4.0, character mode access to BANNER will be terminated a few weeks before the upgrade, on August 13. (Note that the upgrade will *not* affect your ability to access BANNER-related information via DuckWeb.)

Here are the minimum desktop computer configurations you'll need for GUI access to BANNER:

1. **Windows 95 / 98 / NT:**

   Pentium-class PC

   64MB RAM (**96MB or more recommended**—see "Newer Operating Systems and Browsers Require More RAM" on page 6)

   20Mb free disk space
   15-inch display

2. **Macintosh OS 7.5.5 / 8.x / 9.x :**

   Power Mac G3 / G4

   64Mb RAM (**96MB or more recommended**—see "Newer Operating Systems and Browsers Require More RAM" on page 6)

   300Mb free disk space (for Windows software)

   15-inch display

   Windows 95 / 98 / NT emulation software, such as SoftWindows 5.x or Virtual PC 2.x / 3.x

We encourage everyone to begin using GUI access to BANNER as soon as possible. The sooner you start, the easier the final transition will be.

Questions?

For additional information and questions, please contact Jim Bohle (**346-1706**, *jbohle@oregon*) or Susan Hilton (**346-1725**, *hilton@oregon*).

Network Services Substantially Reduces Fast Ethernet Charges

At the end of January, Network Services substantially reduced its charge to activate a jack for 100Mb Fast Ethernet, lowering the rate from $250 to $150.

The cost of activating a 10Mb Ethernet jack will remain unchanged at $100 each, but bulk-rate discounts will continue to be available for jobs requiring 10 or more connections at a time.

If you have questions about these or other network services on campus, or if you wish to request network service for your department, see **http://ns.uoregon.edu/** or call **346-4395**. If you wish to inquire about the Ethernet capability in your building, send email to *nethelp@ns.uoregon.edu* .

Two New Search Engines Expand Your Options

If you're looking for alternatives to the many search engines that are already out there, you might want to take a look at **www.oingo.com** and **www.allthesites.com**.

Oingo is a new "meaning-based" search engine that goes beyond searching for just simple text characters. With *oingo*, you can refine your search based on the actual meaning of your search words and phrases.

Allthesites, while employing more traditional character-based search modes, claims to be the world's largest, fastest search engine. It currently has over 300 million URLs in its database.

Intel Donates

UO computing labs, departments benefit

Celeron Processors

Intel Corporation recently donated a large number of Celeron 366MHz processors to the University of Oregon. This generous gift is being used to upgrade slower Celeron/PII-based systems in university computing labs and departments.

Product Details

Format. Celeron 366s are PPGA form factor, but should work in Slot 1 boards with an adapter. (Adapters are not included, and if required would cost approximately $10.)

System Compatibility. These processors are compatible with Celeron, PII-, and PIII-based systems. However, they will *not* work with 486 or Pentium/Pentium MMX systems.

Terms of Use

These processors are intended only for direct use by university departments and labs. No individual, personal, or resale/trade use is permitted.

How to Request Processors for Your Department/Lab

Many of the processors have already been distributed, but some are still available. If your lab or department can benefit from a Celeron upgrade, send an email request to Joe St Sauver (*joe@oregon*) as soon as possible. In your message, indicate the number of processors you require and their intended use.

We sincerely appreciate Intel's continued interest and generosity to the University of Oregon.

Help Keep Computing Accounts Current by Updating HRIS Information

Prior to disabling campus computing accounts, the Computing Center first checks the data stored in the Human Resource Information System (HRIS). Unfortunately, this information is not always accurate—and without accurate information, we can't ensure that some computing accounts won't mistakenly be disabled.

It's particularly important that the following staff have an active HRIS record:
• courtesy /associate appointments
• adjunct faculty / part-time instructors
• temporary support staff

Without an active record, these staff members will appear to be unaffiliated with the university and their accounts will be disabled during our end-of-term accounting process. In addition, certain staff records require special handling:

• adjunct faculty or part-time instructors who are not currently teaching but who will return at a future date need to maintain current status

• courtesy or associate appointments with expiration dates need to be renewed

• people working on contract who are not paid through payroll need to establish a courtesy or associate status

Please assist us by updating university employee information in HRIS. This will ensure that university employees will have uninterrupted access to their computing accounts. If you have questions concerning HRIS updates as they pertain to computing accounts, contact Mary Bradley (*mbradley@oregon*, **346-1737**).

Trends in State Research/ Higher Ed Networking

The Computing Center recently prepared a 12-page document summarizing the current state of Statewide Higher Education Research and Education Networks and State Agency Networks. The document reveals several trends:

• Virtually all namesake state universities now have Internet2 connectivity, with Abilene being far more common than the vBNS.

• In roughly 80% of all states, the state higher education research and education network runs a physical statewide backbone.

• With only a few exceptions, state government agencies either are customers of the higher education research and education network, or operate a separate state agency network. It's very uncommon for higher education to be customers of a state agency network.

To get an Adobe Acrobat copy of this document, go to **http://darkwing.uoregon.edu/~joe/state-networks.pdf**

After Modem Pool Upgrade, Problems

Hervey Allen
*Microcomputer
Support Specialist*

hervey@oregon.uoregon.edu

Last February, we upgraded the UO modem pools with new Cisco equipment and consolidated them at 346-6520 (see "UO Modem Pools Consolidated" at the bottom of the following page).

While this upgrade has benefited most users, a few have had problems connecting. Some people reported problems getting their existing setups to work as well as before. Either they couldn't connect at all, or their connection was inexplicably slow.

In almost every case, the problems we've seen were related to WinModems or modems that did not properly support standard protocols. If you're troubleshooting a modem problem, the first place to look is in one of these two areas. Remember:

1. We support standard protocols *only* (this means V.90—not X2, KFlex, V.FC/V.Fast, etc.)

and

2. WinModems/host-based modems continue to have all sorts of problems (see "WinModems: A No-Win Situation?" in the Winter 2000 issue of *Computing News*, http://cc.uoregon.edu/cnews/winter2000/winmodems.html)

With these facts in mind, here are some typical problems we have seen and their possible solutions:

1. Problem:

A SupraFAXmodem previously connected without problems; it now connects much slower or not at all.

Possible Solution:

The modem may be using V.FC/V.Fast to connect. This protocol is no longer supported.

Try going to the Supra/Diamond Legacy support web pages at **http://www.diamondlegacy.com/** to see if there is an update for your modem. If not, you'll need to use an AT command to tell the modem to connect using V.42bis (try ATF17), or at 14,400 bps. As far as we know, there is no upgrade from V.FC to V.34 (28,800 bps) for these modems.

Note: Use of AT commands for modems differs for each operating system and type of dialin software. The exact AT command required also differs; you should be able to find it in your modem manual.

If you need help with AT commands, you can contact Microcomputer Services at **346-1412**. Because of the complexity of the AT command solution, however, you may find that a new modem will serve you better.

2. Problem:

You have a K56Flex and/or X2 modem, but not a V.90 modem. The modem either no longer connects, or it connects at a slower speed.

Possible Solutions:

Go to the modem manufacturer's web site to see if there is a software update for your modem.

Each manufacturer or modem model has a different process for applying these software updates. On some WinModems, you'll need to update the drivers installed under Windows. On non-WinModems, you often need to update the modem's internal code ("flash the firmware") on the modem to effect a change.

Note:

- 3Com now owns US Robotics. Try **http://www.usr.com** to find software for legacy US Robotics modems.

- Mac users of US Robotics modems may need to download a special tool from the USR/3Com site to determine exactly which modem they have and what update they need.

- Supra modems with K56Flex support that do not have a firmware update may still offer a chip swap program. Call the Diamond/Supra tech support center at (254) 299-2756 and have the correct product ID handy. The last time we called, the support staff indicated they would still send a new chip with V.90 support—but only for Supra modems that don't have a firmware update option.

See Diamond/Supra's web page at **http://www.diamondlegacy.com/** to determine what product you're using.

3. Problem:

You have a modem that supports V.90 and has secondary support for K56Flex and/or X2. It no longer connects, or connects at a slower speed.

Possible Solution:

We've seen multiple modems with V.90 support that don't connect or connect at slower speeds. In general, modems that are relatively new (i.e., modems purchased within the last six to nine months) won't have this problem.

However, many older modems that were flashed to support V.90 do have this problem. This is because some of them first try to connect using X2 and/or K56Flex before they'll try V.90. The problem lies in the way the modem falls back to V.90. Often this is done incorrectly and the whole connection fails.

In most cases, the solution is to go to the modem manufacturer's web site to see if there is a firmware update for the modem. After you apply the update, chances are the modem will connect correctly. The update will often make the modem first try V.90 and/or it will install an improved fallback mechanism.

Alternatively, you can often use AT commands to force the modem to con-

Surface for WinModems, Some Older Modems

nect using V.90 instead of X2 or K56Flex.

4. Problem:

You have a WinModem/Host-Based modem that was connecting, but which now fails to connect.

Possible Solutions:

There are many reasons why this may be happening. Perhaps the WinModem is trying to connect using K56Flex and/or X2. In such cases, updating the modem driver is often the fix.

The problem with WinModems is that applying the update can be anywhere from trivial to incredibly complex depending on the manufacturer. Even worse, many WinModems are essentially unsupported, and no updates are available.

Some WinModems do such a poor job of negotiating connections that turning off this feature can get them connected. (But note that if this works, you have no error correction—which means you will probably drop your connection pretty quickly.) If doing this, or connecting at much slower

speeds gets you in, then it may be time for a new modem. You will definitely want to see if there is a driver update for the modem.

5. Problem:

You were dialing in without problems, but now you get repeated prompts to enter the password.

Solution:

What's happening here is that our modem pool now correctly supports the ability for Windows to prompt you several times if you have entered your password incorrectly in the original dialup box.

If you enter a password incorrectly three times, the connection is dropped. We consider this a plus because it gives you several chances to type your password correctly before losing your connection.

In every case, people who called to complain that they were inexplicably getting the multiple password prompt had either changed their modem password without realizing it, or they had inadvertantly typed it incorrectly. (A

typical error is accidently leaving NUM LOCK on when typing a password.)

Summary

Most of the problems I've described affect only older modems that don't support V.90 correctly, or inexpensive modems that make poor connections/don't correctly support standard communication protocols.

For the majority of modem users, there are definite benefits to our modem pool upgrade and consolidation. First of all, the modem pool is now larger. This means you have a better chance of being able to connect during peak times. In addition, the lines cost less, and our modems are much more reliable and are easier to configure and maintain.

Need Help?

If you need help checking for WinModem updates or downloading files, contact the Microcomputer Services staff (*microhelp@oregon*, **346-4412**), or stop by their office in Computing Center Room 202.

UO Modem Pools Consolidated

Get in the habit of dialing 346-6520

José Domínguez
Senior Network Engineer
jad@ns.uoregon.edu

On February 28, 2000, Computing Center network engineers completed the consolidation of our modem pools. The V.90 modems served by 346-6520 and 346-3565 are now in one large pool of 288 modems at **346-6520**.

The old modem numbers (346-3565, 346-1586, 346-2150) will continue to be forwarded to the new pool

until next fall. After that, they will be removed from service.

Continued expansion: On March 9, a new pool of 76 V.90 modems was put into service at **346-5975**. These modems are connected through AT&T.

In the future, we plan to migrate all our modem pool services to AT&T connections, which should be less expensive and allow for future expansion. Funding has already been approved to expand the modem pool to a total of 576 by fall of 2000.

To see current modem usage statistics, go to

http://ns.uoregon.edu/

and open the "Network Monitoring" link.

Newer Operating Systems and Browsers Require More RAM

Minimum requirements continue to rise

Hervey Allen
Microcomputer Support Specialist
hervey@oregon.uoregon.edu

"Is my machine broken?" We often hear this question from people who try to run Netscape 4.0.6+ or Internet Explorer 4.*x* on their desktops and find that pages either load *very* slowly or not at all.

"But all I want to do is browse the web! Why do I need to upgrade my machine just for that?" These days, "just browsing the web" takes a lot more memory and TCPU than it used to—and the same is true of the newer operating systems. Unfortunately, you can't avoid upgrading simply by sticking with an older browser, because older browsers can't cope with the increasingly complex web environment.

Consider the following examples:

Windows 98 Second Edition. This needs a LOT of memory and TCPU! Many people with 32MB and 48MB machines actually thought their machines were broken because they either performed very poorly or became unreliable. It really looks like you need 64MB or more to run this OS with any reliability on many machines.

Netscape versions 3.04 and below get Javascript errors left and right. For example, almost every page on CNN will give you a Javascript error. On Mac OS 8.6, we were able to replicate type 3 errors and crashes. On Mac System 7.1, we got type 1 errors and crashes while browsing such web sites.

Netscape 4.0.5 and earlier and IE 3.0.2 and earlier have expired certificate issues. The older the browser, the worse this is. In some cases you cannot proceed to view the page or finish a transaction.

Because web sites are becoming more complex and are increasingly used for interactive transactions, upgrading your equipment is ultimately unavoidable. **Even to use DuckWeb— an essential information resource for UO students—4.*x* series browsers are recommended for best performance.**

Yes, you can get older PCs, Macs, and browsers to work in some cases, but the support overhead is high and the user's experience will be frustrating at best. Furthermore, the minimim requirements can only continue to rise.

Summary

To reiterate, you'll need Netscape 4.0.6 or IE 4.x or higher to browse web sites like CNN and DuckWeb, or for some online transactions. Office 98 on the Mac and Office 97 or 2000 on the PC also require more RAM and processing power.

In short, the bar has been raised. Microcomputer Services now recommends the minimum configurations outlined in the table below.

Current Minimum Requirements

Operating System	Memory	Machine
Windows 2000	128MB RAM	Pentium II 300 Mhz or higher. (Yes, this is really true! We ran Windows 2000 on a Pentium II 300 with 96MB of RAM and it was *slooooow*.)
Windows 98 (2nd Edition)	64MB of RAM (96-128MB RAM if you want to use Office *and* a browser)	Pentium class or higher
Windows 95	32MB RAM (48-64MB RAM if you want to use Office 97 or above *and* a browser; 64 MB RAM recommended)	Pentium class or higher
Mac **Bare minimum:**	32MB RAM (48-64MB RAM if you want to use Office 98 *and* a browser)	PowerMac running Mac OS 7.6.1
Recommended Minimum:	64MB RAM or more	PowerMac or higher running Mac OS 8.1

MacTCP No Longer Works Reliably in Modern Network Environments

Mac users are advised to upgrade to Open Transport

Hervey Allen
hervey@oregon.uoregon.edu

Last January, people using older Macintosh computers occasionally experienced difficulties accessing off-campus Internet sites. The only machines affected were Macs that still use the MacTCP (or "Classic") style of network software.

These incidents underscored the fact that MacTCP is a very old and inadequately supported implementation of the TCP/IP protocol, which is used for Internet access by such applications as Netscape, Telnet, email programs, FTP, and USENET News.

Why Is MacTCP Becoming Obsolete?

When MacTCP was last updated, some features available in the TCP/IP protocol were still not in widespread use, but lately advanced network features are becoming more common. One such feature is the ability to "mark" network traffic to give it priority for applications such as Voice Over IP (VOIP)—i.e., phone calls via the Internet. At some point this service may become integral to the UO campus.

To implement a service like VOIP, a feature called Type of Service (ToS) is often set for some packets on our network. In January, one of our network service providers turned on this feature. When they did this, MacTCP Macs, which fail to implement this part of the TCP/IP protocol correctly, could no longer connect to any site that was accessed via this provider.

The problem is a direct result of MacTCP's inability to fully support features in the TCP/IP protocol, the protocol used for Internet access by such applications as Netscape, Telnet, email programs, FTP, and USENET News. For the time being, this problem has been resolved by artificially resetting certain ToS bits for all incoming IP traffic at the UO. However, this is only a short-term solution and problems with MacTCP are likely to recur with increasing frequency as time goes on.

In short, in the future no version of Apple MacTCP can be relied upon to work correctly as newer networking features are implemented.

No MacTCP updates are forthcoming. We have contacted Apple directly, and they have confirmed that Apple will not develop an update for MacTCP to resolve this issue. (MacTCP was last updated in 1994 and has been considered a legacy product for several years.)

This means that sooner rather than later, all MacTCP Macs *must* be upgraded to use Open Transport. (While it's also possible to install a third-party patch, we don't recommend it.)

How Can You Tell if You're Using MacTCP?

If you can access the Internet on your Mac, go to the Apple menu, choose the Control Panel, and look for "MacTCP." If it's there, that's the network protocol your Mac is using. If instead you see a control panel called TCP/IP, your Mac is using Open Transport.

Recommended Upgrades. If you're using MacTCP, you'll need to upgrade your Mac operating software by January 1, 2001, when our network "quick fix" will be retired. Both our short- and long-term upgrade recommendations are listed below:

• **Short term:** Mac OS 7.6.1 *(minimum)*

• **Long-term:** PowerMac with 64+ MB of RAM and Mac OS 8.1 or above

Note that current UO students, faculty, and staff may obtain Mac OS 8.1 at no cost from the CC Public Domain server on UOnet, and the Documents Room has a CD to lend.

Where to Get Help

Because this problem is quite complex, the Microcomputer Services staff has created a web page explaining it in depth. This page,

http://micro.uoregon.edu/macintosh/ mactcp.html

lists all your options, memory requirements, machines for which there is no solution (e.g., any 68020 Mac, like an SE or Plus), our recommendations, and much more. Please read it carefully before directing questions and concerns to our staff.

If you still have questions after reviewing the information on our web page, email a consultant at *microhelp@oregon*, or call **346-4412**.

SSL Encryption Lets You View Your Email Securely on DARKWING or GLADSTONE

Hervey Allen
hervey@oregon.uoregon.edu

Email correspondence via DARKWING and GLADSTONE is a little bit more secure now that Computing Center systems staff has tested and installed new encryption software on these systems.

The new software, known as SSL (Secure Socket Layer) can encrypt your username and password when you check your email and can also encrypt all your messages when you download them to a local machine (or when you read them using IMAP mode). This technique is formally known as POP over SSL or IMAP over SSL. (POP and IMAP are two methods your email client uses to connect with DARKWING or GLADSTONE when you read your email.)

How do POP and IMAP work? Generally speaking, POP (Post Office Protocol) physically transfers mail from the host to your machine, giving you the choice to leave a copy on the host as well. With IMAP (Internet Message Access Protocol), your email stays on the server and you read it (via your network connection) from your desktop machine. In both cases, your username and password are passed back to the host to verify your identity, after which the data for each message is sent to your machine.

How does Secure Socket Layer (SSL) encryption work? SSL takes your plain text data and scrambles it in such a way that it could not be read if someone were "listening" in on your session, or on the network in general.

The nice thing about this method is that it's virtually invisible. After you've configured your email client with SSL, you'll notice very little difference, ex-cept perhaps for a slight slowdown on modem connections.

Which Email Clients Support SSL?

Current versions of Outlook support both POP and IMAP over SSL, while Netscape's email client supports only IMAP over SSL. Eudora currently has no SSL support.

Outlook. In Outlook you can generally choose to use SSL by going to the Tools menu and opening "Accounts..." Click the Mail tab, highlight your email account, choose properties, and click the "Advanced" tab. Then check the box labeled, "This server requires a secure connection (SSL)."

Note: Exact menu placements of this option may vary between versions of Outlook.

Netscape. In Netscape, click on the Edit menu and open "Preferences..." Then go to the Mail & Newsgroups category and choose Mail Servers. Highlight the incoming mail server, click Edit, click the IMAP tab, and then check the box labeled, "Use secure connection (SSL)."

Note: These preferences are not available in Netscape if you're using POP mode to get your email.

I don't see these options…what now? If you don't see the options described above in your Outlook or Netscape email programs, you'll need to upgrade to a current version.

Port settings. We are using standard ports for both these services (995 for POP and 993 for SSL), so you do not need to change these settings in your email clients.

Outgoing Email is Insecure

One thing to be aware of is that SSL does *not* encrypt email that you send out. However, the good news is that hackers are most often interested in surfing, and the most critical information is usually your username and password.

The only way to ensure that your email is encrypted from start to finish is to use something like PGP (Pretty Good Privacy). This method is a bit more involved.

If you're interested in using PGP, you can start reading about it on the International PGP web pages at **http://www.pgpi.org/** Be sure to read the online FAQs (Frequently Asked Questions) files to get an understanding of how things work.

You might also want to read *PGP: Pretty Good Privacy* by O'Reilly Associates for detailed information about the product. The book is available for checkout from the Documents Room (205 Computing Center). For a complete overview of the book, see

http://www.oreilly.com/catalog/pgp/

Questions?

If you have additional questions about how to use POP or IMAP over SSL, contact Microcomputer Services in Room 202 of the Computing Center (*microhelp@oregon,* **346-4412***)*. The office is open Monday through Friday from 9am to 5pm.

Better Safe than Sorry: Safeguard Access to Your Computer Account

Recent Hotmail security breaches on campus underscore the need for protection

Steve VanDevender
Academic UNIX Systems Manager
stevev@darkwing.uoregon.edu

Some software—e.g., email services like Hotmail, Eudora, and Microsoft Outlook, an FTP client, or modem dialup software—offers you the choice of storing your GLADSTONE, DARKWING, or OREGON password to streamline access to your account.

While the convenience may be tempting, you should avoid doing this unless you can ensure that you have exclusive access to that computer system. Whether you're working on a public computer or your own desktop computer at home, you are still vulnerable.

For example, if you set up Hotmail to retrieve mail from your GLADSTONE, DARKWING, or OREGON account and store your account password in your Hotmail profile, you're running a significant risk of password theft. Hotmail has had a series of well-publicized security problems involving theft of Hotmail account profiles, and since millions of people use Hotmail it is a tempting and profitable target for attacks. We've already seen a case in which a UO student's GLADSTONE account was accessed without her knowledge or permission, apparently because someone obtained her password from her Hotmail profile.

Recording your account password on a public lab computer may expose it to other people who use the same computer later. If you share your computer with roommates or keep your computer where visitors can easily access it, you may also run the risk of having someone discover one of your stored passwords.

We strongly recommend that you safeguard your personal computer with some kind of password protection. Require a password for deactivating a screensaver or for booting and accessing your computer, and don't otherwise expose your computer to random use.

Many people wonder why they should take steps to protect their exclusive access to their GLADSTONE, DARKWING, or OREGON accounts, saying "I don't keep anything important there, so I'm not worried about anyone else being able to get at my files." In the majority of cases investigated by our system administrators, intruders don't want access to your account to look at what you have in it. Instead, they use stolen accounts to mount security attacks against university systems and others on the Internet, or to illegally exchange copyrighted software with others—often without your knowledge and without obviously interfering with your normal use of your account.

Should you be the unwitting victim of one of these attacks, you could temporarily lose access to your account while the situation is being resolved. So take the time to protect your account password; this one small step can go a long way toward preventing major headaches later on.

WEB AUTHORS: PUT *.htaccess* TO WORK FOR YOU

Jon Miyake
Academic Services Consultant
miyake@darkwing.uoregon.edu

If you're a web author, you'll probably want to add *.htaccess* to your toolkit. *.htaccess* is a tool that gives you the means to personalize your web site. With *.htaccess*, you can control access to your site, define error messages and MIME-types (content-types) of files, redirect browser requests—and much more.

While standard system definitions cover most of a web author's requirements, there are times when they're not sufficient—and that's when *.htaccess* can be especially useful. For example, suppose you want to put a file on your web site for users to download. If this file has a unique file extension (i.e., an extension not recognized by the system configuration), it will download as indecipherable visual "garbage." To fix this, you can use *.htaccess* to properly define the MIME-type for that unique file extension.

.htaccess is also useful for defining error message files that are specific to your web site. Whereas the default error messages returned by the local web server merely provide a generic response indicating that a problem was encountered with a requested file, *.htaccess* allows you to generate much more useful information. With *.htaccess*, you can create detailed, site-specific error messages and even provide a means for users to send you feedback about dead links.

If you're interested in learning how to use *.htaccess*, see the tutorial at **http://cc.uoregon.edu/consult/htaccess/**

Be Aware of Security Issues

The very features that attract users to ICQ also make it vulnerable to attack

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

*(**Editor's Note:** The Computing Center does not recommend using ICQ, nor do we provide support for it. However, we do feel it's important to point out some of its vulnerabilities because we know that there are ICQ users at the UO.)*

ICQ, an Internet instant messaging application, has been widely used on the Internet for years. The program allows users to send short messages, files, and other communications swiftly and easily over an Internet connection.

Unfortunately, ICQ's design makes it very susceptible to attacks from unscrupulous people on the Internet. The very features that attract users to ICQ make it an easy target. Because of its ease of use and overall simplicity, ICQ is used by Internet marauders as a channel for attacking computers, spreading viruses, stealing files, and generally wreaking havoc with innocent users of the program.

Personal information unprotected. When you register ICQ and begin using the program, it collects a certain amount of information about you: your name, email address, geographic location, and other optional information from the registration process. This information is stored on the ICQ servers and is available to anyone on the Internet.

A casual search through the ICQ database can elicit quite a bit more information than you might want to give to strangers. This excess of information can lead to harassment, stalking, and annoying "prank" messages sent by Internet outlaws. (These same bad behaviors are prevalent in all forms of Internet communication, but the wealth of information available through ICQ makes these abuses all the more frequent.)

IP information exposed. Along with your personal information, ICQ also sends out detailed and potentially damaging Internet Protocol information with each message you create. Your ICQ User Identification Number (UIN) and your Internet Protocol (IP) address appear in the header information for each message.

This IP address is the unique identifier for your computer on the Internet. Ordinarily, your IP address is relatively hard to find and your computer is less likely to be noticed by attackers. But because ICQ publishes your IP address along with your messages, attackers can readily determine your IP address and recognize that you're running ICQ.

Who's Most at Risk…and Why

If your Internet connection is through a modem, the possibility of someone launching an attack on your computer is relatively slight. *People connecting to the Internet through Ethernet here on campus or through cable modems and DSL connections at home are much more vulnerable.*

You should also be aware that Ethernet and other high-speed connections keep the same IP address information for days, weeks, or months at a time, giving would-be abusers a stable target for an attack.

When you register ICQ and begin using the program, it collects a certain amount of information about you…This information is stored on the ICQ servers and is available to anyone on the Internet…

Because there are some well-defined security holes in ICQ's protocols, attackers can use this information to gain access to your machine. In addition, illicit programs tailored to ICQ users are available on the Internet that can scan a particular machine's network ports for vulnerability. An attacker can use one of these programs, identify your computer's vulnerabilities, and exploit them.

Damage Potential

Once attackers have worked their way into your computer through one of these insecure network ports, they can download and read your files. Anything in your ICQ program directory is pretty much an open book to a determined attacker. The extent to which attackers can access the files on your computer depends on the method they use to break into your machine. Still, a good rule of thumb is that if they have access to any part of your computer, they can access **anything** on your computer.

with ICQ Instant Messaging

Identity theft. One important file of interest to attackers is the settings file used by ICQ itself. Although most of the file is encrypted, the password used by ICQ is saved as clearly readable text. Once that password is known, abusers can change your password on the ICQ servers, then contact anyone on the Internet and make threats, promises, deals, and mischief *in your name*. They could also download and use your ICQ contact list, any files or information that the ICQ servers might have stored about you, and generally cause you tremendous problems.

File tampering. In addition to taking files **from** your machine, abusers can also put files **onto** your machine with even more devastating results. There's a whole shopping list of "back-door" applications—programs that run in the background on your computer, unseen and undetected. These programs can allow totally free access to your computer.

Once the back-door program is in place, attackers can see what you're working on, move files to and from your computer at will, modify your computer's settings… anything they like. More importantly, they can then use your computer as a platform for launching similar attacks against other computers on your network.

Virus infection. In addition to back-door programs, an attacker could also install viruses and other destructive programs to disrupt the operation of your computer.

Malevolent attachments. Quite apart from the security holes in the ICQ protocols, there are also security breaches in the way that ICQ handles files.

When you first install ICQ, you can accept file transfers from any other ICQ user. Depending on the security level you have set, ICQ may accept and open these files automatically. This is a widely used method for installing back-door programs. The file is sent as an attachment or file transfer, often with an innocuous-sounding name like "Fluffy Bunny Screensaver.exe." The unsuspecting user runs the program, and perhaps even sees a series of fluffy bunnies parading across the screen.

Meanwhile, behind the scenes, a back-door program is installing itself, configuring itself, and alerting its creator of a newly opened computer to exploit. These same sorts of vulnerabilities exist in email in general, as well as in downloading files through a web browser.

Another twist on this file transfer exploit is if you, the ICQ user, allow downloaded files to automatically open themselves, the back-door programs could be installed automatically without your ever having to touch the files at all. *Needless to say, choosing to automatically open downloaded files is a very bad idea!*

Security Tips

Here are a few steps you can take to safeguard your computer against attack:

• **We strongly recommend that you do *not* use ICQ or other instant-messaging programs.** All of these instant messaging programs have security holes and related problems. Use standard email for your communications. Email has much fewer security holes and can be safeguarded more easily.

• **Don't download files from strangers, and don't open any files at all unless you know the person who sent them, you were expecting that particular file, and you have an up-to-date virus checking program running to catch any suspicious activities that installing a back-door program or virus might cause.** Norton Antivirus 2000 is available to all UO students, faculty, and staff on the Duckware CD-ROM.

• **If you must use ICQ, download and install the most current version** (currently Version 99b Beta v.3.19). Download only from a reputable site, like **http://www.icq.com**. There are modified versions of ICQ on the Internet that act like the regular ICQ program, but run back-door services as a part of their installation.

• **Set your security in ICQ to allow *only* the transactions you want.**

• **Require your authorization for people to add you to their contact lists.**

• **Check the box that says "Do not publish IP address."** (Available only in the most current versions)

• **Set the security level to "High."** You'll need to type in your password more frequently, but your ICQ environment will be more secure.

• **Do not save your password.** This will force you to type in your password every time you open ICQ, but it will make your password less vulnerable to marauding hackers.

If you follow these simple procedures, you'll be more protected against outside attacks.

It's up to you to make your computer safe. Use the ICQ settings shown on the following page to ensure that you've minimized the possibility of attack.

Need More Information? See

http://www.icq.com

http://www.wired.com/news/news/technology/story/12758.html

http://blacksun.box.sk/icq.html

ICQ Security Issues, continued…

Recommended ICQ Settings

1. File Transfer Configuration

Open the Events tab and configure File Transfer in the Events dialog box. Notice that

- "Auto Receive Files" is **<u>unchecked</u>**
- "Always Overwrite Existing Files" is **<u>unchecked</u>**
- "Pop Up Response Dialog" is **checked**
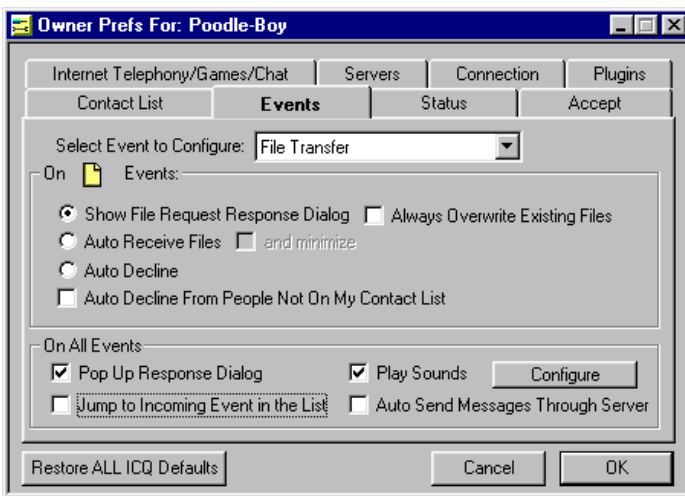
2. Security Preferences

In the box below, notice that

- "My authorization is required" for changing ContactList Authorization
- "Do not publish IP address" is **checked**. *(This option is available only in the latest versions of ICQ.)*
- "Save Password" and "Web Aware" are **<u>unchecked</u>**
- "Security Level" is set to **High**
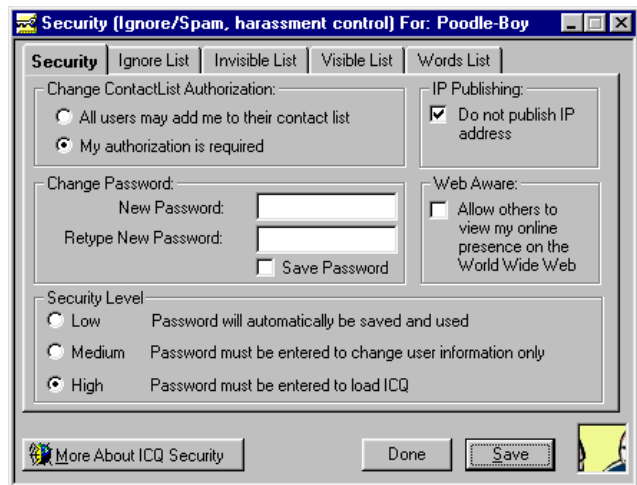
The Ugly Truth About 'PrettyPark.Worm'

Dan Albrich
Microcomputer Network Specialist
dalbrich@oregon

In recent weeks, Microcomputer Services consultants have been seeing quite a few instances of a new Windows virus called PrettyPark.Worm.

PrettyPark.Worm was originally spread by email from a French email address. Once the virus program is executed, it tries to mail itself automatically to all the email addresses registered in your email address book. In addition, it tries to connect to an IRC server and join a specific IRC channel to obtain system information, ICQ identification numbers and nicknames, and your email address and Dial Up Networking name and password.

If you want to know more about this virus, including repair and prevention information, see Symantec's AntiVirus Research Center page at

http://www.symantec.com/avcenter/venc/data/prettypark.worm.html

You can also get help by contacting Microcomputer Services in Computing Center Room 202 (*microhelp@oregon*, **346-4412**). The office is open Monday through Friday from 9 am to 5 pm.

Be forewarned that virus issues can be extremely difficult to deal with. The most common fix is for Windows 95/98 only. If you have a Windows NT machine, or an infection that's not easily resolved, troubleshooting can take quite a long time. The charge for checking in your machine for an extensive repair is $60/hour.

Practice Safe Computing. For continuous protection, always run Norton AntiVirus Auto-Protect and use LiveUpdate to make sure you have the latest virus definitions. Be suspicious of executable file attachments (for example, .exe, .shs, MS Word, or MS Excel files), especially ones from newsgroups or unknown sources.

Check Out the New UO Home Page!

See what's new at www.uoregon.edu

On February 4, after many months of planning, designing, and tweaking, the new UO home page made its debut.

The major redesign of the UO site began last summer, shortly after the Computing Center hired web specialist Dave Ragsdale. Ragsdale, formerly the multimedia-Internet development specialist at the University of Nevada in Reno, set to work creating design proposals, and a special oversight committee was formed to guide the redesign process. Committee members included Tom Hagar and John Crosier (Office of Communications), Joanne Hugi and Joe St Sauver (Computing Center), George Beltran (University Publications), Martha Pitts (Admissions), Robert Felsing (Knight Library), and Computer and Information Science student Chun-Chih Chen.

The committee reviewed a total of 16 designs and narrowed their choices to three favorites, reaching a final consensus in November. Ragsdale spent another month paring down file sizes and adjusting links, and the design was unveiled to President Frohnmeyer and the UO Communications Council in January.

The result of this concerted effort is a makeover that retains many of the popular features of the old site, such as the weather link and photograph of the day, while introducing new useful features like a prominent link to WebMail and a link to personal pages.

Other notable features include the "UO News and Facts" section (a comprehensive resource for basic information as well as the latest news and events on campus), a new electronic campus directory (see "New Electronic Student/Staff Directory Coming Soon" on page 20), and the "Featured Web Page," which showcases a different campus site each day.

To ensure consistency throughout the site, second- and third-level pages employ the same green and gold colors and elements of the UO seal as the home page.

The new design has been well received overall, and comments poured in from both on- and off-campus immediately following its debut. "I like it!" "Very nice new page!" were typical responses. Some also expressed particular appreciation for the new WebMail link and the prominent display of the UO's directory number at the foot of the page.

Templates Available

Campus departments interested in incorporating the UO home site's new look in their own site designs may use the templates and instructions provided at **http://cc.uoregon.edu/uotemplates** If you would like further guidance in adapting these templates to your particular site, feel free to contact Dave Ragsdale (*dave@oregon*).

Web Tip: If you're interested in learning more about how to make your web site more visible, see the latest tips at **http://micro.uoregon.edu/tips/sitevisibility**

Dealing with 'Outliers': How to

Neither ignoring unusual data values nor deleting them at will are good solutions. Here are some suggestions for keeping your data—and your conclusions—on track

By Robin High
Statistical Consultant
robinh@darkwing.uoregon.edu

It's an unfortunate fact of life that data are not well-behaved. "Outliers"—unusual data values—crop up in most research projects involving data collection.

This is especially true in observational studies where data may naturally have unusual values, even if they come from reputable sources. Data entry errors or rare events (such as a thermometer left in the sun, a change in accounting practices, or a subject who has a sudden muscle spasm)—all these and many more are reasons for outliers to exist in a dataset.

Likely Sources of Outliers

Data errors. When looking for the source of outlying observations, first check for data recording or entry errors. To reduce the occurrence of data recording errors, use a spreadsheet program such as EXCEL for data entry.

With large datasets, computer programs can be written to identify data entry errors. SAS is a particularly good tool for this purpose.

"Rare" event syndrome. Another reason for outliers is the "rare" event syndrome—extreme observations that for some legitimate reason do not fit within the typical range of other data values. Such unusual observations might include

• a 70 degree day in January in Oregon
• a 500 point rise/drop in a stock market index
• an unusually high score on an aggressiveness scale for a troubled child

All these events may be quite unusual, but they're still part of the overall picture.

Why Are They a Problem?

Developing techniques to look for outliers and understanding how they impact data analysis are extremely important parts of a thorough analysis, especially when statistical techniques are applied to the data.

For example, in the presence of outliers, any statistical test based on sample means and variances can be distorted. Estimated regression coefficients that minimize the Sum of Squares for Error (SSE) are very sensitive to outliers.

There are several other problematic effects of outliers, including

• bias or distortion of estimates

• inflated sums of squares (which make it unlikely you'll be able to partition sources of variation in the data into meaningful components)

• distortion of p-values (statistical significance, or lack thereof, can be due to the presence of a few—or even one—unusual data value).

• faulty conclusions (it's quite possible to draw false conclusions if you haven't looked for indications that there was anything unusual in the data)

The following example may seem a bit extreme, but real data with this feature actually exist. The results vividly demonstrate the potential problems that lurk in the background due to unusual data values.

	Sorted Data					Median	Mean	Variance	95% Confidence Interval for the mean
Real Data	1	3	5	9	12	5	6.0	20.0	[0.45 to 11.55]
Data w/ Error	1	3	5	9	**120**	5	27.6	2676.8	[-36.630 to 91.83]

The first four data values across each row contain the same numbers. However, in the second row, the fifth entry has a large discrepancy when compared to the value in the first row. Note that in the presence of one outlier, the median does not change in this example.

The median is called robust (i.e., it usually does not vary greatly) in the presence of a small number of outliers and is often the preferred summary statistic for the "center" of a skewed distribution. Notice how just one outlier can greatly distort the mean, variance, and 95% confidence interval for the mean. Similar results apply to regression, analysis of variance, or any technique that uses sums of squares in the calculations.

How to Detect Outliers

The "normal" distribution myth. For many statistical modeling purposes, input data do not necessarily require a "normal" or symmetric, bell-shaped distribution. (This

Maintain Your Data's Integrity

feature applies primarily to residuals from a statistical model—a subject for future articles.) Discrete data or counts, by definition, will not usually look very "normal."

In fact, for data to be used in linear regression model, the independent or explanatory variables should *not* have a normal distribution. It can be demonstrated mathematically that normality is not required nor even desirable for this type of data. What is important is to check for data values that lie well outside the range of other data (called leverage points) that can have a undue influence on the results. Your objective should be to collect data with a distribution that allows you to make the best inferences possible about the population under study.

Visual aids. Check the distribution of data values by levels of a categorical variable, if available. This procedure should always be one of the first steps in data analysis, as it will quickly reveal the most obvious outliers.

For continuous or interval data, visual aids such as a dotplot or scatterplot are good methods to examine how severe any outlying observations actually are. A boxplot is another very helpful tool, since it makes no distributional assumptions nor does it require any prior estimate of a mean or standard deviation. Values that are extreme in relation to the rest of the data are easily identified.

Univariate tests check for the presence of outliers; however, many of them are designed to check for the presence of only one outlier, and they also make distributional assumptions which are often not relevant (e.g., they assume a normal distribution when you have very skewed non-negative data). They often require that a location (mean) or scale (standard deviation) parameter be estimated from the data. As shown earlier, outliers can greatly affect their values. This is one reason why "eliminating data that exceed two or three standard deviations" may not be a good, or even a reasonable, rule of thumb.

IQR computation. It is quite simple to compute the inter-quartile-range (IQR) and then use a multiple of it as a number that defines what values are considered outliers. A boxplot uses this technique to identify outliers. Using a boxplot is an extremely effective approach, especially when working with large datasets that have continuous data.

One way to implement an IQR computation is to use PROC UNIVARIATE with SAS and save the order statistics available with its OUTPUT statement. The first quartile (q1), third quartile (q3), and inter-quartile range (IQR) can be saved in an output file. You can use them to flag observations that lie outside of q1-(1.5*IQR) and q3+(1.5*IQR) as potential outliers and anything outside of q1-(3*IQR) and q3+(3*IQR) as problematic outliers.

Multivariate outliers can also lurk undetected in an analysis. Univariate tests for outliers are not designed to identify multivariate outliers. For two data values, x1 and x2, neither one may be considered a univariate outlier when looked at with a univariate test as described above.

However, the combination of their two values can lie outside the periphery of the range of data in two-dimensional space—in this case the two values are called an influential or leverage point that, for example, can exert a strong impact on the computation of regression coefficients.

multivariate outliers

X2

(most of the data plots here)

X1
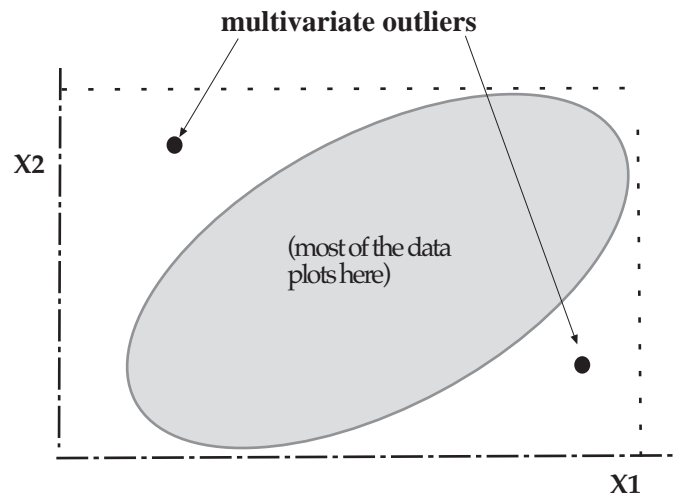
What Should You Do About Them?

Effectively working with outliers in numerical data can be a rather difficult and frustrating experience. Neither ignoring nor deleting them at will are good solutions. If you do nothing, you will end up with a model that describes essentially none of the data—neither the bulk of the data nor the outliers. Even though your numbers may be perfectly legitimate, if they lie outside the range of most of the data, they can cause potential computational and inference problems. Some possible approaches to working with outliers are listed below.

Transformation. Transforming data is one way to soften the impact of outliers since the most commonly used expressions, square roots and logarithms, shrink larger values to a much greater extent than they shrink smaller values. However, transformations may not fit into the theory of the model or they may affect its interpretation. Taking the log of a variable does more than make a distribution less skewed; it changes the relationship between the original variable and the other variables in your model. In addition, most commonly used transformations require non-negative data or data that is greater than zero, so they are not always the answer.

Outliers, *continued...*

Deletion. Only as a last resort should you delete outliers, and then only if you find they are legitimate errors that can't be corrected, or lie so far outside the range of the remainder of the data that they distort statistical inferences. When in doubt, you can report model results both with and without outliers to see how much they change.

Data transformations and deletion are important tools, but they shouldn't be viewed as a cure-all for distributional problems associated with outliers. Transformations and/or outlier elimination should be an informed choice, not a routine task.

Accommodation. One very effective plan is to use methods that are robust in the presence of outliers. Nonparametric statistical methods fit into this category and should be more widely applied to continuous or interval data. When outliers are not a problem, simulation studies have indicated their ability to detect significant differences is only slightly smaller than corresponding parametric methods. There are also various forms of robust regression models and computer intensive approaches that deserve attention.

Summary

Despite the difficulties, exploring why outliers exist can provide many clues to the development of better models. In fact, many great discoveries in human history can be traced to a researcher exploring some outlying or unusual value. Outliers may indicate that an important range of the data has been ignored that is worth knowing about.

This article only skims the surface of dealing with outliers. It's presented with the hope that looking for unusual data values will become a regular part of your analysis, and that your research objectives and knowledge of your subject matter will help you decide what to do with them once you find them. The "common sense" test is often the best solution.

Always apply exploratory data analysis techniques that look for both univariate and multivariate outliers and then evaluate their impact on the results. This will help you reach conclusions that are in line with your research objectives.

Need More Information? For a more detailed explanation of outliers, as well as a bibliography of references, see
http://darkwing.uoregon.edu/~robinh/outl.txt

Napster/Napster-like Programs Not Music to All Ears

Napster's program for downloading/ distributing music online concerns some universities

Napster, a popular program designed to facilitate searching, downloading, and distributing music online in CD-quality MP3 format, has recently become a cause for concern at some universities.

The program is available at **http://www.napster.com/** for Windows 95/98/NT; and alternative implementations of "Napster-compatible" programs are also available, including "open source" Napster-compatible clients for Amiga, BeOS, Java, Linus, and MacOSX (see **http://opennap.source-forge.net/**)

Why the Concern?

Most student residence halls at major universities now have student-controlled systems with direct network access. In addition, most major universities have high-bandwidth Internet access circuits, which make them desirable to those seeking a well-connected server from which to download music of interest.

Napster is a cause of concern for some universities because of two considerations:

1. Students logged in on their university network accounts may use Napster to search for, and download, music. Because multimedia files are comparatively large, Napster activity can add a significant amount of traffic to a university's inbound Internet load.

2. Students may use Napster to distribute MP3-format music that they've stored on their personal computers—without regard to copyright law. Dis-

tributing copyrighted material without the consent of the copyright holder is of course illegal.

University Responses

Some universities have reacted to Napster by attempting to block it in a variety of ways, such as

• educating their students about the problem and asking them to voluntarily refrain from using Napster—an appeal that is often ignored

• reconfiguring local name servers to disassociate napster.com from its usual server address (easily overridden when users change the name server they rely upon)

• blocking access to TCP/IP ports traditionally used by Napster (not foolproof, since Napster is designed to search for an alternative open/unfiltered port if the default Napster is blocked, and OpenNapster clients can be configured to use virtually any arbitrary port)

• blocking access to the network address blocks assigned to napster.com at the university's border routers or institutional firewall (also not foolproof because external proxy servers can circumvent these blocks, and OpenNapster servers can be pointed arbitrarily at servers anywhere on the Internet)

None of these ploys is adequate to resolve the problems Napster poses for the university community. Moreover, Napster is only one of a growing number of similar file sharing applications, and there is no one-size-fits-all solution for dealing with them. For example, the Napster-like program iMesh (**http://www/imesh.com**) operates on entirely different software, using entirely different network addresses and network ports. Even if Napster were disabled, programs like iMesh would continue to operate without interruption.

Why are These Programs So Difficult to Limit?

Napster and related programs are difficult to control for a number of reasons:

1. Popularity. These programs facilitate easy access to music—and music has extremely broad appeal.

2. The stigma of "censorship." Any effort to restrict access to online resources is customarily denounced as "censorship," with concomitant negative media attention. It's difficult to succinctly explain complicated technical issues in the brief "sound-byte"-length opportunities provided for rebuttals.

3. Increasingly sophisticated anti-filtering technology. These programs often include effective mechanisms for circumventing filters that are deployed to stop them.

4. Contact between the party requesting a particular file (the client) and the party providing access to that particular file (the server) is brokered rather than being arranged directly. However, the central brokering server doesn't actually participate in the file transfer—thereby avoiding problems of network congestion at a single central point, and eliminating any possibility that the central server can be accused of copyright violations itself.

What's the UO Doing About Napster?

The UO continues to closely monitor Napster usage and will continue to cooperate fully with law enforcement authorities when copyright infringements are reported.

SPRING 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 full range of computer and Internet training, from novice to advanced skill levels. These information technology ("ITC") workshops are free and open to currently enrolled students, as well as staff and faculty.

There is no registration; just show up a few minutes before the scheduled start. All seating is available on a first-come, first-served basis. You must meet the workshop prerequisites as stated in the description. If fewer than five people are present ten minutes after the scheduled start, the workshop may be canceled or rescheduled at the discretion of the instructor.

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** (email: *cbell@darkwing.uoregon.edu*).

Note: The Summer ITC Schedule will be available June 12

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.

Basic Computing and Software Skills

Endnote/Procite: **What Are These, and Why Should I Use Them?**

Learn how to use bibliographic software. New this term is the ability to connect to the UO Library Catalog and transfer citations directly from the catalog into either EndNote or ProCite.

	Mon Apr 17	3:30 - 4:50pm	RSR	Brownmiller, Lenn
	Thu Apr 20	12:30 - 1:50pm	RSR	Brownmiller, Lenn

Communication & Research Topics

Net a Job: Use the Web - ▶ **Prerequisites (*To register for this workshop, contact the UO Career Center at 346-3235*)**

Link up to thousands of jobs, internships, employers, companies, and organizations. Learn how to submit your resume electronically. Basic working knowledge of the web required.

	Tue May 2	3:30 - 4:50pm	EC	Haynes

Introduction to Powerpoint (Windows and Macintosh)

Create dynamic lectures or presentations with Microsoft PowerPoint. This hands-on introduction will help you learn how to use PowerPoint to organize your lecture, quickly turn a simple outline into a colorful slide show or a set of visually effective overheads, create course handouts and notes, and add graphics and charts to make your point.

	Tue May 2	2 - 3:50pm	ITC	Heerema

* WORKSHOP LOCATION CODES *

EC: Electronic Classroom (Windows)	144 Knight Library
ITC: Macintosh Classroom	267B Knight Library
RSR: Reed Seminar Room (Windows)	235 Knight Library

★ **Requires an active account on** DARKWING **or** GLADSTONE

SPRING WORKSHOPS

Workshop	Day/Date	Time	Location	Presenter

Basic Web Publishing Skills ★ - ▶ Prerequisites

Web Publishing I
This workshop teaches you the HTML elements you need to create a basic web page, and shows you how to publish it on the web. Requires familiarity with a graphical web browser (e.g., Netscape Navigator) and an account on DARKWING/GLADSTONE. You must know your username and password.

	Mon Apr 10	2 - 3:50pm	EC	Benedicto
	Fri Apr 21	10 - 11:50pm	ITC	Frantz

Web Publishing II
Prerequisites: Web Publishing I or equivalent knowledge and skills, and an account on DARKWING/GLADSTONE. You must know your username and password.

	Mon Apr 10	2 - 3:50pm	EC	Galbraith, Laliberte
	Fri Apr 28	10 - 11:50am	ITC	Falbo, Galbraith

Web Publishing III
Prerequisites: Web Publishing II or equivalent knowledge and skills, and an account on DARKWING/GLADSTONE. You must know your username and password.

	Mon May 1	2 - 3:50pm	EC	Johnson

Web Publishing Beyond the Basics ★ - ▶ Prerequisites

Cascading Style Sheets (*http://darkwing.uoregon.edu/~jqj/inter-pub/css/*)

	Fri May 19	10 - 1:50am	RSR	Johnson

Web Design Principles and Practices (*http://darkwing.uoregon.edu/~cbell/design/*)
Requires Web Publishing I and II or equivalent knowledge and skills

	Mon May 8	2 - 3:50pm	RSR	Bell

Web Graphics (Requires Web Publishing I, II, and III or equivalent knowledge and skills)

	Wed May 10	1 - 2:50pm	ITC	Kim

Web Programming I
Brief introduction to using scripts to generate web pages dynamically. Some computer programming and UNIX knowledge desirable.

	Fri May 5	10 - 11:50am	RSR	Johnson

Web Programming II
Basic introduction to using Javascript to generate web pages dynamically. Some knowledge of computer programming and UNIX desirable.

	Fri May 12	10 - 11:50am	RSR	Johnson

Workshops Available on Video

Looking for an alternative to the workshop format? The Computing Center Documents Room (Room 205) has a growing collection of videos on using computers and computer software. You can use your UO picture ID to check out these videos. For a list of available titles and descriptions, visit ***http://micro.uoregon.edu/workshops/*** Call **346-4406** for more information.

Library Adds New Proxy Server:

UO off-campus users now have improved access to the Library's web-based electronic resources, thanks to the addition of a new proxy server that acts as an intermediary between an off-campus computer and the Library's online resources.

You'll find instructions on how to use the UO Library's proxy server at **http://libweb.uoregon.edu/systems/proxy/**

New Electronic Staff/Student Directory Coming Soon

If you're looking for the very latest campus address information for UO staff and students, try using the new online directory. The directory will soon be available from the Directory link on the UO home page at **http://www.uoregon.edu** (see "Check Out the New UO Home Page!" on page 13).

The new directory is the work of the Computing Center's Auxiliary Services programming staff, who developed it in collaboration with the Telecommunications Department. Unlike the old directory, which relied on periodic updates to stay current, the new directory pulls up-to-date information directly from the university's BANNER database. This ensures that the information is the most current possible, as any corrections and modifications to BANNER data will be instantly reflected in the directory.

The table below outlines some of the basic differences between the old and new directories. If you have further questions about the new BANNER-linked directory, contact Susan Hilton (*hilton@oregon*).

Feature:	Old Directory	New Directory
Who's listed?	Most computer account holders on campus, plus anyone listed in periodic data dumps from BANNER and participating departmental systems	Those who are in BANNER, plus departmental entries
Which email addresses are shown?	All the user's UO computer account email addresses on campus. No additional external email addresses.	The user's preferred email address as it is stored in BANNER. Can include external email addresses.
Home address/phone	No	Yes (for students) unless directory restricted
Link to user web pages	Yes	No
Search capability	Can search for any text	Searches name fields only
Wildcards searching	Yes	No (stemming only)
Job Title	Yes	No
Clickable "Mail to:" links	Yes	No
Anti-spam address harvesting technology	Yes	Yes
Time to search for an unusual last name	Fraction of a second	About a second
Time to search for a common last name	Fraction of a second	Several minutes

Proxy Servers, Auto Discovery, and IE 5

Recent developments in the world of proxy servers may affect the way you browse the web

Hervey Allen
hervey@oregon.uoregon.edu

As you may already know, proxy servers are machines that speed your browsing time by storing local copies of web sites you visit frequently. This means that after you first access a site, you no longer have to wait for a page to load from a very remote or slow web server. Instead, web sites you've already visited load quickly from the local proxy. The proxy server also updates pages each time you revisit a site, to ensure you'll see the latest version.

Why Use a Proxy Server?

Speed. The major advantage of using a proxy is that it saves time and bandwidth. For modem users in particular, a proxy server can increase the speed of page retrieval dramatically.

Security. Another advantage is increased security. Because traffic going back to your machine appears to come from the UO proxy server, it's harder for hackers to find its true location. This protects your machine against typical security attacks, and it also makes it more difficult for anyone to track you for profiling or advertising purposes.

WPAD Changes the Proxy Picture for IE5 Users

Last July, a new mode of identifying proxy servers, called the "Web Proxy Auto-Discovery Protocol," or "WPAD," was introduced.

The advent of the WPAD protocol impacted computing at the UO because Microsoft decided to employ it in Internet Explorer 5. We quickly discovered that had we *not* decided to implement certain key pieces of WPAD, campus users of Internet Explorer 5 (which is included by default with Windows 98 2nd Edition and Windows 2000) would

have experienced very long delays when they tried to use Internet Explorer's default configurations.

Furthermore, part of the WPAD protocol includes the use of a machine named "wpad.*domain*" (e.g., in the UO's case, "wpad.uoregon.edu"). This practice poses a potential security threat, as described below.

IE5/WPAD Security Loophole. The following scenario illustrates the potential security problem inherent in the WPAD protocol:

• By default, Internet Explorer (read Windows 98 2nd Edition and Windows 2000) will look for **wpad.uoregon.edu** on the UO campus. If it finds this machine, it *assumes* it's a valid proxy server.

• Because it might be possible for others to create a proxy server under the name **wpad.uoregon.edu** if we didn't create a server by that name, unauthorized parties could use their falsely identified proxy to get data from user sessions—and if they wished, they could also use it to capture secure information like encrypted credit card data. **(Note that we do not use our proxy server for secure transactions.)**

The setup for all this is actually more complicated. For instance, you can also use the UO proxy server for FTP sessions, or you can give clients pointers to the proxy server when they start up using DHCP records. This subject is too involved to discuss in detail here, but you can obtain a thorough explanation by pointing your web browser to **ftp://ftp.nordu.net/internet-drafts/draft-ietf-wrec-wpad-01.txt**

WPAD at the UO

Considering the number of campus users who have Internet Explorer version 5, we felt it was important to implement the WPAD protocol to ensure that these users would not experience unacceptably slow start-up times.

Consequently, we created a **wpad.uoregon.edu** alias that points to our proxy machine **proxy.uoregon.edu**.

This solution ensured that everyone already using our proxy server saw no change in service, and those who chose the default network settings for Internet Explorer 5 did not experience slowdowns.

How to Tell if You're Using the UO Proxy Server

If you're using Internet Explorer 5, you can see if you're using the UO proxy server by following these steps:

1. Go to the Start menu in Windows

2. Choose Settings

3. Choose Control Panel

4. Open the Internet Options control panel

5. Click on the Connections tab

6. Click on the "LAN Settings…" button in the LAN settings section of the Connections section

7. If the box "Automatically detect settings" is checked, you are using the UO proxy server. This can be quite misleading because there is a "Proxy server" section on the same screen that you can use if you want to manually configure your proxy server settings, and many people assume that if this is not filled out, a proxy server will not be used.

Note: *If you uncheck the box "Automatically detect settings" and click on OK twice to close the control panel, the next time you use Internet Explorer you won't use the UO proxy server.*

Need More Information?

If you have further questions about proxy servers, or how all this works, be sure to read the WPAD protocol document at **ftp://ftp.nordu.net/internet-drafts/draft-ietf-wrec-wpad-01.txt**
Or, you can contact Joel Jaeggli at *joelja@darkwing.uoregon.edu*

For general client configuration questions or troubleshooting, contact Microcomputer Services at **346-4412** or *microhelp@oregon.uoregon.edu*. You can also visit them on the web at **http://micro.uoregon.edu**, or in person in Room 202 Computing Center.

# Wide Area Bandwidth Questions

Joe St Sauver
joe@oregon.uoregon.edu

This article attempts to answer some common questions about the capacity and performance of OWEN/NERO, the consortia that provides Internet public connectivity for higher education, public K12 and State of Oregon agencies.

One of the most common questions we hear is, "Is the OWEN network currently operating at its peak capacity?" This is a tricky question, because OWEN adjusts the size of its Internet transit capacity to satisfy observed peak inbound capacity requirements. OWEN also monitors (and will adjust) its internal intrastate backbone circuits if required, although those circuits currently have sufficient reserve capacity to meet forecast needs.

Our Transit Bandwidth Profile

OWEN/NERO's current UUNet transit bandwidth profile as of late January 2000 looked like this:
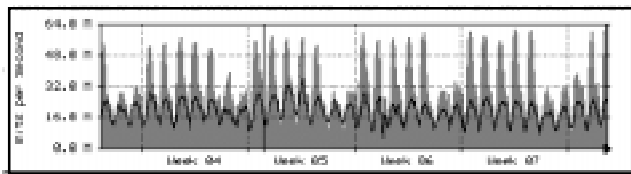
The tall peaks represent inbound (Internet-to-us) circuit utilization, and the lower line represents outbound (us-to-Internet) circuit utilization. The horizontal axis represents time, with each spike being roughly a day apart. The vertical axis is traffic measured in Mbps (megabits per second). This is a very typical graph for OWEN/NERO transit connectivity, and we can learn some important things from it:

• **Use tends to peak dramatically during the day, with the greatest peaks occurring during early to mid-afternoon.** Use also exhibits periodicity associated with the day of the week.

• **Generally speaking, inbound use dominates outbound use, and inbound use determines the amount of transit bandwidth we require** (inbound and outbound capacity can't be independently provisioned at different levels).

• **Usage is not "flat topping."** If we were grossly underprovisioned, usage would typically exhibit a characteristic "flat top/plateau" area leading up to, through, and immediately after the period of peak demand. We're confident that we're obtaining the actual capacity we've purchased from UUNet, and that we haven't "overpurchased" capacity we don't currently require to meet peak demand.

Sizing our transit circuits to meet inbound peaking loads is clearly the key. If we buy more capacity than we need, we'll spend more than we should—and for no benefit (we can't "warehouse" excess network capacity; if we can't use it, it's simply lost…a wasted expenditure). If we buy less capac-ity than we need, particularly less than we need to meet peaking loads, the network will perform poorly and our customers will become dissatisfied.

"How about establishing a bandwidth standard per user, and provisioning bandwidth accordingly?"

People sometimes suggest provisioning our bandwidth according *to* a *per-use* standard. The theory behind this is that such a standard would tend to cap (lower) OWEN/NERO's bandwidth requirements. Once you "run the numbers," it becomes clear why we don't have such a standard:

OPEN (one of OWEN/NERO's customers) has 530,000 students. We know that OUS has just over 60,000 students. Let's assume there are roughly 10,000 DAS agency employees who have access to OWEN/NERO (we believe this number is grossly low; however, for the sake of argument and for the convenience of using round numbers, let's go with that estimate). Totaling that up, OWEN/NERO services roughly 600,000 users.

OWEN/NERO has 121 Mbps worth of commodity transit bandwidth, 76 Mbps from UUNet and 45 Mbps from Cable and Wireless (CWIX). If you divide the 121,000,000 bits per second of bandwidth by our estimate of OWEN/NERO's 600,000 users, that works out to:

$$\frac{121,000,000 \text{ bits per second}}{600,000 \text{ users}} = \text{roughly 200 bits per second per user}$$

Note that dialup modem connects users at 56,000 bits per second ("56 Kbps"). Clearly, 200 bits per second is a very modest level of commodity bandwidth by any standard, far below what would potentially be required if we were to guarantee even modem level throughput to all OWEN/NERO customers. But what if we were to approach this problem in reverse, computing the committed bandwidth we'd need to provision if we were to guarantee every user minimum simultaneous access at modem-like speeds of 56,000 bits per second? Doing the math for that, we obtain:

(600,000 users) * (56,000 bps) = 33,600,000,000 bps or 33,600 Mbps

That's 277 times the current OWEN/NERO bandwidth—financially unfeasible and technically unrealistic.

Finally, suppose we ask, "What would OWEN/NERO's budget be if every person serviced by OWEN/NERO paid a dollar a month[1] for their Internet connectivity?" The number is a rather staggering $7,200,000/year, far more than the roughly $1,500,000-$2,000,000/year that OWEN/NERO currently spends.

Bottom line? OWEN/NERO delivers world class connectivity at a bargain price.

---

[1] **Note:** *AOL and most other Internet service providers offer service at $15-$20/user/month; however, they offer a variety of value-added services over and above the network access that OWEN/NERO provides. We chose the dollar/user/month figure as a value representing only the network connectivity part of a typical user's monthly Internet costs— although obviously that number could vary for a given user or provider.*

Did You Know...?

TIPS FROM THE COMPUTING CENTER HELP DESK

▶ **You can access your email almost anytime, anywhere, from a web browser by using WebMail.**

If you're looking for more flexibility, try this convenient alternative mail client. WebMail is accessible from the new UO home page at www.uoregon.edu / Or you can go directly to

https://webmail.uoregon.edu/

Note: Because some mail clients move messages around as they're read, it's important that you pick—and stick with—a single email client to avoid problems. So if you do decide to use WebMail, don't attempt to use it in conjunction with another mail client, such as Pine or Eudora.

▶ **Your Ed Tech Fees help pay for...**

- Campus computing labs and departmental computing facilities (In 1999, over $800,000 in ed tech funds were distributed to campus schools and departments for the enhancement of their educational technology facilities and services)
- Email and Internet access for all students
- Electronic classrooms
- Computer training and support services

▶ **The Duckware CD gives you network and antiviral software, web tools, shareware, utilites, drivers—and more! It's free and it's available at...**

- Computing Center (Rooms 202 and 205)
- CC-EMU, CC-Klamath, and CC-Millrace Microcomputing Labs
- Knight Library / Science Library Information Technology Centers

COMPUTING CENTER GUIDE

Computing Center Web Site
http://cc.uoregon.edu/

Microcomputer Services
(Room 202)

- 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/hr, $1^{1/2}$ hr. minimum)

346-4412
microhelp@oregon.uoregon.edu
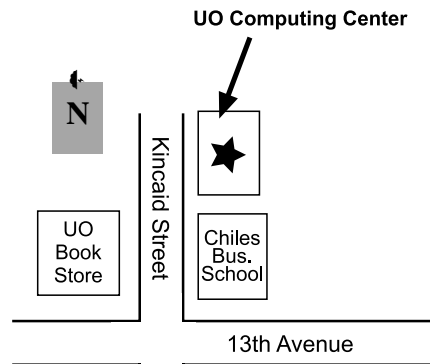*http://micro.uoregon.edu/*

Large systems consulting
(Rooms 233-239)

- VMS, UNIX (GLADSTONE, DARKWING, OREGON)
- statistics packages
- email

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

UO Computing Center

N

Kincaid Street

UO Book Store

Chiles Bus. School

13th Avenue

Documents Room Library
(Room 205)
346-4406
http://darkwing.uoregon.edu/~docsrm

Electronics Shop

For computer hardware repair, installation, and upgrade services, call **346-4403** or write *hardwarehelp@oregon.uoregon.edu*

Network Services

Provides central data communicaiton networking services to the UO community.

346-4395
nethelp@oregon.uoregon.edu
http://ns.uoregon.edu

Modem Number

Dialin modem number for UOnet, the campus network:

- V.90   **346-6520**

Computing Center Hours

Sunday	9 am - 8:30 pm
Monday - Friday	7:30 am - 8:30 pm
Saturday	9 am - 4:30 pm