

COMPUTING NEWS

SUMMER 2004



A view of one of the main buildings of the Oregon Institute of Marine Biology (OIMB) in Charleston, Oregon. OIMB is the permanent home of the University of Oregon's marine biology program, which is open year-round. The campus has facilities for teaching and research as well as student dormitories.

IN THIS ISSUE...

Email

- Oregon Phase-Out Continues3
- What Happens to Your UO Email Account Over the Summer?.....3
- Gmail and the New Extra Large Free Email Accounts.....7

Microcomputing

- How to Improve Your Modem Connectivity2
- A Simple Way to Burn Cross-Platform Discs Under OS X4
- Campus Maclabs, PClabs Groups Share Insights4
- Recycling E-waste.....11
- Renting vs. Buying Music Online.....14
- Some Things You Need to Know about Spyware19
- Computer Conundrums Got You Down?.....23

Large Systems

- Rediscovering the Shell Prompt..... 20

Networking

- NSRC Continues Its Cooperative Ventures Abroad.....8

Security

- Five Essential Steps for Protecting Your PC.....11
- Security Alerts12
- Late-Breaking Security Alerts15
- NFSv4 and NFS Security.....18
- New Books on Security in the Docs Room.....21

Statistics

- Getting Started with SAS's PROC MIXED16

People

- Joanne Hugi Retires5
- Jim Bohle's SEVIS Work Earns Praise 6

Interesting Sites

- Cybercrime in the News10
- Sites Worth Seeing22

- IT Workshops.....5

How to Improve Your Modem Connectivity



Sometimes slowing your connection speed can actually improve your connection!

Dan Albrich

Manager, Microcomputer Services
dalbrich@uoregon.edu

If you connect to the UO network via dial-up modem and are either experiencing slow connectivity, connections that drop, or are completely

unable to connect, you may wish to try slowing down your modem.

That's right, in some cases slowing down the modem's connection speed will actually improve your connection!

This tactic is particularly effective when the modem is experiencing errors due to line noise. Imagine your modem connection to be a conversation between two people, and line noise to be a loud train whistle that causes words to be lost to the receiver. If the speaker is talking very fast, more words are lost than if the speaker is talking slowly over the same time interval. This oversimplifies the issue, but it gives you a general idea of why slower communications are easier to sustain, even given the presence of line noise.

Modern modems also have the capability to change speed during communication, adjusting to transient line noise by speeding up when the noise is not present. This process is called retraining. Unfortunately, in the real world this feature can actually slow you down, or cause the connection to drop entirely.

For example, your modem connects at 26,400, notices a small error rate, and decides to retrain (speed up) to 28,800. At this speed it observes an unacceptable rate of error and retrains back to 26,400. The problem occurs when the modem starts looping between these two speeds, and the only communication that's occurring is that required to retrain (i.e., your data is not being transmitted).

In this scenario, you would experience more reliable—and effectively faster—connections by setting the ceiling connect speed at 26,400 “baud” (or bits per second).

OK, How Do I Slow Down My Modem?

Macintosh Users: On the Mac, modem speed is controlled with the modem setting. In OS X, go to System Preferences → Network → Modem. (If Ethernet is selected as the connection method, you must use the drop-down menu to select the modem first). Slowing down your modem is as easy as selecting “Apple Internal 56K Modem (v.34)” instead of “Apple Internal 56K Modem (v.90)” or (v.92).

Windows Users: Microsoft Windows users need to manually type a modem initialization string, using the following procedure:

- Open the modems (or “Phone and Modems”) control panel.
- Double-click on your modem, then select “Advanced.”
- Find the box labelled “Extra Settings... Extra initialization commands”. In that box, enter **+MS=V34**

Please note that if your modem does not support this particular command, it may fail to dial the next time you try to connect. If this occurs, remove this setting (or change it).

Although the **+MS=V34** command will work on many modems, some models will require a different specific initialization string. For example, all Supra models can use **F17** as the string to slow them down, and all US Robotics modems can use **&U1&N12**.

If these strings don't work with your modem, contact Microcomputer Services for assistance (**346-4412**, microhelp@lists.uoregon.edu). Note that in order to help you, we will need to know which modem you have (in Windows, you'll find this information under the “Phone and Modems” control panel).



UNIVERSITY OF OREGON

COMPUTING CENTER

COMPUTING NEWS

VOL. 19 #3

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

© University of Oregon 2004

Contact: Joyce Winslow
jwins@uoregon.edu

Photography: Dave Ragsdale
dave@uoregon.edu

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

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



Got Extras?

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

Update on Oregon Accounts: Preparations for Phase-Out Continue

In preparation for the Oregon mainframe's phase-out late in fall term, Computing Center staff are continuing to help Oregon users make the transition from Oregon to Darkwing or Gladstone. We're pleased by the progress that's been made to date, and we will continue to help users move their email and other files off Oregon through fall term. (Please note that administrative users on Daisy and Donald are not affected.)

If your computing account is still on oregon.uoregon.edu, here's a list of resources to help you make the transition from Oregon to Darkwing or Gladstone:

1. Do-it-yourself instructions (for all but faculty emeriti):
<http://cc.uoregon.edu/cnews/fall2002/mailmove.html>
(*Note to faculty emeriti:* instead of following these instructions, please contact Lucy Lynch at postmaster@lists.uoregon.edu for help.)
2. Details on the Oregon system phase-out:
<http://cc.uoregon.edu/cnews/fall2002/oregonout.html>
3. Special tips for list owners:
 - "The Great Change." Tools to help you manage various facets of the migration: <http://darkwing.uoregon.edu/~majordom/great-change.html>
 - "Moving Day." Five easy steps for moving your email to Darkwing and updating your list subscriptions:
<http://darkwing.uoregon.edu/~majordom/moving-day.html>
4. Questions? Contact Lucy Lynch at postmaster@lists.uoregon.edu

CC COMPUTING LABS SUMMER SCHEDULE

Open-access campus computing labs administered by the Computing Center are now on their summer schedule:

CC-EMU Lab (22 EMU, 346-1769)

Monday - Friday 7:30 A.M. - 8 P.M.

Closed Saturday and Sunday

CC-Klamath Lab (adjacent to B13 & B25 Klamath Hall, 346-4781)

Monday - Thursday 8:30 A.M. - 7 P.M.

Friday 10 A.M. - 4 P.M.

Closed Saturday & Sunday

CC-McKenzie Lab (101 McKenzie Hall, 346-0787)

Monday - Thursday 8:30 A.M. - 10 P.M.

Friday 10 A.M. - 4 P.M.

Sunday 1 P.M. - 9 P.M.

CC-Millrace Lab (113 Millrace I; 346-0316)

Monday - Thursday 8 A.M. - 8 P.M.

Friday 10 A.M. - 4 P.M.

Sunday 5 P.M. - 9 P.M.

For a map of campus computing labs, see http://cc.uoregon.edu/labs_map.html

What Happens to Your UO Email Account Over the Summer?

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

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

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

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

What if you graduate? After you graduate, you will normally get one free "vacation term" before your account is deactivated. In addition, the UO Alumni Association now offers a free email alternative. Go to <http://alumni.uoregon.edu/> and select the "Free Alumni Email" link for more information.

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

A Simple Way to Burn Cross-Platform Discs Under OS X

Michael Rebar, Ph.D.

*Research Assistant, Institute on Violence and Destructive Behavior
mrebar@darkwing.uoregon.edu*

Have you ever wanted to burn a cross-platform CD on an OS X Mac and find you don't have Toast or Nero installed? DISC-O is a freeware utility for OS 10.3 that can create and burn ISO CD disc images. Here's what the main application window looks like:



To create a new ISO disc image, type a name for the image in the "ISO Image Name" field, then select a source folder

using the "Select folder..." button. DISC-O creates an ISO image at the root level of your boot volume. So, if a user entered "disk1," DISC-O would create the "disk1.iso" image as shown below:



DISC-O can also be used to burn other ISO images. Simply place the image at the root level of your hard drive, type the image name in the "ISO Image Name" field, and press the "Burn" button.

DISC-O loosely enforces the naming conventions in the Joliet specification with RockRidge extensions. This means you can't use illegal characters in your file or path names. DISC-O does not enforce directory tree depth limitations. The next version of DISC-O will support the conversion of **.dmg** to **.iso** files.

DISC-O can be downloaded at
<http://darkwing.uoregon.edu/~mrebar/DISC-O.sit>

Maclabs, PClabs Groups Share Insights on Running Campus Computing Labs

If you're responsible for managing or supporting a Mac or PC lab on campus, you'll probably want to know about two new discussion groups that specialize in lab administration issues: *maclabs@lists.uoregon.edu* (for Mac lab staff) and *pclabs@lists.uoregon.edu* (for PC lab staff).

These discussion groups, which were founded by Architecture and Allied Arts computing lab manager Chris Wiesemann, are forums for lab administrators and staff to compare notes, share troubleshooting insights, and keep each other apprised of the latest news in lab maintenance and security techniques.

In addition to online discussions, the groups hold regularly scheduled meetings on campus. Maclabs meetings are held on the fourth Thursday of every month at 11 A.M., and PClabs meetings are held the fourth Friday of every month at 11 A.M. Advance notice of these meetings is posted on the mailing lists.

This summer's meeting schedule is as follows:

Maclabs: 11 A.M. July 22 105 Computing Center
11 A.M. Aug 26 251 School of Music

PClabs: 11 A.M. July 23 Lawrence Hall (*contact Chris Wiesemann for details at 346-2082*)
11 A.M. Aug 27 (location TBA)

To subscribe to either the *maclabs* or *pclabs* mailing lists, send an email to *majordomo@lists.uoregon.edu* In the body of the message, type :

```
subscribe maclabs (or pclabs)
end
```

(Don't include your email address or "real name" in the *subscribe* command; Majordomo will get the necessary information from the headers of your email message. You also do not need to type anything in the Subject: line of your email.)

Joanne Hugi Retiring from Top Computing Center Post

After more than two decades at the helm, Hugi will step down at the end of this year

Joyce Winslow
jwins@uoregon.edu

Joanne Hugi's long and fruitful association with the Computing Center began when she took a student clerical job in the Documents Room Library in 1970. At the time, Hugi was pursuing a master's degree in computer science, business administration, and education at the UO.

After graduating in 1971, Hugi joined the Computing Center user support staff and taught a variety of computer science courses. In 1974 she was appointed Director of User Services, and over the next two decades she rapidly moved up the management ladder to become Director of University Computing and ultimately, Associate Vice President for Information Services.

Over the years, Hugi guided the university's vital information systems through many technological changes and advancements with a clear vision for future computing and networking needs. Her dedication to finding opportunities for the university to enhance its position with respect to telecommunications and networking led to several fruitful partnerships in both public and private sectors, and she never lost sight of her goal



Joanne Hugi, Associate Vice President for Information Services

of providing superior computing and networking support for the UO's instruction, research, and administrative programs.

Under her leadership, the UO won first place in the annual CAUSE competition for "Excellence in Campus Networking" in December 1996, surpassing its peers in the classification of institutions with operating budgets of over \$100 million.

That same year, the Computing Center was a semifinalist in the National Information Infrastructure's annual competition for networking in the "Public Access" category, and in 1997 *Yahoo Internet Life* cited the UO as

the "most-wired" public university in the U.S., ranking sixth among all U.S. universities.

In December 1997, Governor Kitzhaber appointed Hugi to the 12-member Oregon Telecommunications Forum Council, and she has also served on a number of other committees in the local, regional, and national computing and networking communities, including the Network Planning and Policy Advisory Council for Internet2, the Northwest Academic Computing Consortium (which she chaired for five years), the UO's Educational Technology Committee, and the EDUCAUSE board.

Looking back on her career, Hugi is most proud of her contribution to making major Banner administrative software transitions (particularly the move from a mainframe-based to a web-based user interface) as painless as possible, overseeing the growth of the UO's network infrastructure, and guiding the OWEN/NERO network project, which provides high-speed connectivity to state government and K-12 institutions in Oregon. She is also quite proud of her staff. "I'm pleased to have served with such a talented and dedicated staff," she says. "Over the years they have consistently met the challenge of providing superior user services on a shoestring budget."

Hugi's immediate future is filled with travel plans, and she is looking forward to an extended period of globe trotting. First stop: Tuscany in October.

**FREE
WORKSHOPS:
THE INFORMATION
TECHNOLOGY
CURRICULUM**

IT Classes are taking a break this summer and will resume in the fall. Go to

<http://libweb.uoregon.edu/it/>

and tell the staff what topics you'd like to see offered in the future.

International Programs' Staff Salute the UO's SEVIS Module

Bohle's expert programming assistance wins high praise

Joyce Winslow
jwins@uoregon.edu

When new federal regulations went into effect in early 2002, all those responsible for designing and implementing college student information systems had to scramble to meet a reporting deadline that was less than a year away.

Here at the UO, the new mandate had a big impact on the Office of International Programs. Ginny Stark, Director of International Student and Scholar Services, was suddenly confronted with the urgent reality of having to electronically record detailed, current information on over 1000

foreign students, visiting professors, and researchers in a new government database called SEVIS (Student and Exchange Visitor Information System). Could SEVIS be made to work with the UO's existing computing systems? Would her department have to take the expensive step of scrapping its Macintosh machines in order to adapt? Did they have adequate staff to do the job? And finally, could they possibly do everything required of them by the looming deadline?

A self-described "technological novice," Stark speaks with obvious relief of finding help from Computing Center senior analyst and project manager Jim Bohle. Bohle and his team of technical support specialists immediately set to work reviewing SEVIS protocols. They determined that it was possible to modify the UO's Banner environment and other native systems to work with SEVIS, saving the university the many thousands of dollars it would have cost to purchase a new SEVIS-ready package.

As the work began, it became obvious that the Office of International Programs would need additional staff



At a Banner Coordinating Group meeting in June, International Programs' staffers Ginny Stark and Peter Eberhardt surprised Administrative Services' project manager Jim Bohle with a plaque of appreciation.

to coordinate the effort. An entire subcommittee had to be created to handle the recording of student addresses alone, and the need for in-house technical support for the ongoing modifications in SEVIS was also evident. A new position for SEVIS coordinator was created, and several months into the project, Peter Eberhardt was hired to fill that slot. He has worked closely with Bohle ever since.

Both Eberhardt and Stark are unanimous in their praise for Bohle's extraordinary perseverance through the early, difficult stages of working to integrate several disparate systems, computing environments, and technologies on a tight deadline. They are especially grateful for his innovative approach to managing SEVIS' batch process procedure. Bohle's work not only greatly expedited the management of all the various pieces of student information, it ensured timely production of essential documents, without which students could not enter the country and register for classes.

"Jim is the critical support person for the batch process, and he is key to making sure the SEVIS module works locally with each new release of Banner and each new

Jim Bohle for His Role in Implementing

SEVIS modification,” says Eberhardt. Stark is in complete agreement. “Without Jim Bohle, we wouldn’t be nearly as confident of meeting all our responsibilities in regards to SEVIS,” she says.

Bohle himself is modest about his role in the UO’s successful implementation of SEVIS, but his work put the UO in the vanguard of universities striving to adapt their systems to interact seamlessly with the government database. Stark says this became apparent when she compared notes with other universities who called

to find out how the UO had solved its SEVIS-related software problems.

There is no time to rest on his laurels, however, as Bohle would be the first to admit. As he puts it, “SEVIS is a moving target.” Its constant updates keep Bohle, Eberhardt, and the other members of the SEVIS team on their toes, as does the predictable stream of new Banner software releases. The team’s next challenge: getting SEVIS information to automatically update in Banner as students graduate, change addresses, or alter registration status.

Gmail and the New Generation of Extra Large Free Email Accounts

Google, Yahoo, and Hotmail give consumers new choices

Joe St Sauver, Ph.D.

Director, User Services and Network Applications
joe@uoregon.edu

Jumbo-sized web email accounts from a number of vendors will soon be competing for your business. Here’s a brief summary of the new Google, Yahoo, and Hotmail offerings entering the market.

Gmail

Google, already famous for its industry-leading web search service, has now jumped into the free web email market.

If you’re accustomed to a traditional free MSN Hotmail account offering 2MB of disk space, or even Darkwing or Gladstone accounts with 100MB quotas, Google’s free Gmail accounts offering 1000MB worth of space represent quite a paradigm shift, particularly when you couple that headroom with the ability to privately “Google” all that mail.

At this point, you may be asking, “So what’s the catch?”

Well, Gmail *is* supported by advertising, and the ads you’ll be shown if you use Gmail *are* targeted based on your interests. The ads aren’t obnoxious or intrusive, but the advertisements you see do reflect the contents of your mail via an automated ad selection process. For example, if you’re corresponding with friends about travel to Hawaii, don’t be surprised if you see airline airfare specials to Hawaii, or Hawaiian hotel advertising.

Browser support. You should also know that Gmail doesn’t work with all browsers. As of June 24th, 2004, Gmail supported browsers are:

- MS IE 5.5 and later
- Netscape 7.1 and later
- Mozilla 1.4 and later
- Mozilla Firefox 0.8 and later, and
- Safari 1.2.1 and later

Obviously that covers a substantial share of the browser market, but there are some popular alternatives (such as Opera) that aren’t listed yet.

The biggest “problem” with Gmail right now is that while it is still in beta testing, accounts are available by invitation only. Folks who already have Gmail accounts periodically get a number of invitations which allow them to invite a small number of friends to also get Gmail accounts. Of course, as Gmail passes out of its test phase, this issue should disappear.

Other Web Email Providers ...

While Gmail has recently lead the field in offering jumbo-sized email accounts, other web email provider haven’t been standing still. For example:

- *Free Yahoo! Mail* now offers 100MB worth of storage, and if you’re willing to pay, you can get *Yahoo! Mail Plus* with *two* thousand megabytes of storage, POP access, mail forwarding, and other features (<http://mailplus.mail.yahoo.com/help>)
- Beginning in July, Hotmail will reportedly increase its default quotas to 250MB, with its “Plus” service looking much like Yahoo in offering 2000MB of storage for approximately \$20 per year (see “Email Space Race Heats Up” at <http://www.informationweek.com/showArticle.jhtml?articleID=22101948>)

Innovative UO-based Networking Group

In less than a year, the NSRC has participated in workshops and conferences in Ecuador, Nepal, the Netherlands, Tunisia, Italy, Venezuela, Uruguay, and Senegal

Joyce Winslow

jwins@uoregon.edu

The Network Startup Resource Center (NSRC), which has been based at the UO Computing Center since 1996, has been busy as ever providing educational programs and engineering assistance to regional networks around the world.

Since October 2003, various members of the UO/NSRC group have crisscrossed the globe more than half a dozen times to facilitate training workshops on a wide range of networking topics. By the end of July, the group will have participated in two workshops and a network architecture planning session in Ecuador, Internet Corporation for Assigned Names and Numbers (ICANN) meetings in both Tunis and Rome, the Africa Network Operators Group (AfNOG) 2004 workshop in Senegal, and training sessions in Nepal, the Netherlands, Venezuela, and Uruguay.

By sharing information, equipment, and technology, the NSRC aims to help develop regional Internet infrastructure for collaborative research, education, and international partnerships. Building from a three-year core grant from the National Science Foundation, it has developed strategic alliances with many partners in industry and academia to support its activities, establishing an extensive base of contacts willing to contribute time and expertise to help develop national and regional networks in Africa, the Middle East, Latin America and the Caribbean, the New Independent States, the Asia/Pacific region, and some educational network systems in the U.S. Below is a brief summary of recent and upcoming NSRC activities:

Ecuador. The workshops in Ecuador are designed to help develop Ecuador's national research and education network. When operational, this network will be useful to such research projects as the magmatic activity study currently underway by UO seismologists in cooperation with Ecuador's Escuela Politécnica Nacional.

The first of these hands-on training workshops was held in late February at a university outside of Quito; the next series is scheduled for July 26 to 31. Contributors to the February workshop, which focused on system administration and IP services, included NSRC instructor Hervey Allen, Maria Dolores Lizaraburu (an Ecuadoran



photo by Amanda Thomsen

Nancy Dotse hands out course texts to AfNOG workshop participant Djintangar Golmadingar. With the support of O'Reilly Books, Cisco Press, Prentice-Hall, and Addison-Wesley, the NSRC has been able to donate thousands of technical reference books to establish technical libraries in regional universities and emerging network organizations worldwide.

who works part time for the NSRC project), UO network engineer Carlos Vicente, and longtime NSRC volunteer and supporter Brian Candler. Instructors for this summer's wide-area network routing, monitoring, and security workshop in July will include UO network engineers José Domínguez and Carlos Vicente, as well as Mike De Leo of Cisco Systems.

In December 2003, UO/NSRC representatives also participated in a meeting organized by the Organization for American States (OAS) in Quito. UO Director of Network Services Dale Smith and NSRC project manager Steve Huter joined peer professionals in the region to share ideas on formulating science and technology policies and strategies for the hemisphere—particularly in the areas of information technology and communication and advanced networks and cyber infrastructure. Other major topics under consideration were cooperative strategies for nanotechnology, biotechnology, clean technologies, and renewable energy.

Continues Its Cooperative Ventures Abroad

Nepal. NSRC instructor Hervey Allen will serve as a track leader at this summer's South Asia Network Operators Group (SANOG) workshops, a non-profit forum for data network operators in South Asia. Workshop topics include Linux system administration, network security, web services, the Domain Name System (DNS), and running large mail servers using Exim.

With assistance from the NSRC, SANOG organizes regional training programs for academic and commercial network operators in Afghanistan, Bangladesh, Bhutan, India, Maldives, Nepal, Pakistan, and Sri Lanka.

Netherlands. Computing Center support specialist Lucy Lynch, together with NSRC project manager Steve Huter and the Internet Society's Mirjam Kuehne, coordinated the DNS/ccTLD registry workshop in Amsterdam, which ran from June 18 through June 22. Its aim was to provide technical training to the operators of country-code top-level domains (ccTLDs) who are managing servers and services for their national registries, and to foster relationships with colleagues in the industry.

Senegal. UO/NSRC participants in the fifth annual meeting of the Africa Network Operators Group, which was held in May, included Computing Center support specialist Joel Jaeggli, NSRC project manager Steve Huter, and instructor Hervey Allen.

A forum for technical coordination and cooperation among African Internet Service Providers and academic/research network engineers, AfNOG first came into being in 1999 with the assistance of the NSRC. Its aim is to provide technological training and education for network operators who are developing the continent's network infrastructure and Internet services, and to foster stronger international cooperation. The NSRC is currently working with regional networking groups to help establish a pan-African regional registry (AfrinIC).

Venezuela. Computing Center senior network engineer José Domínguez was the lead instructor for the routing and advanced services track at the WALC 2003 workshop in Merida, Venezuela, last October. Topics for this track included BGP, IPv6, multicast, and VoIP.

The NSRC operated a virtual routing lab for the workshop from the UO Computing Center and also loaned equipment and facilitated the donation of technical reference books for participants.

This fall at WALC 2004 in Cuzco, Peru, José will again be teaching the routing/infrastructure track, this time with the support of UO/NSRC colleague Carlos Vicente.

Uruguay. The NSRC has worked closely with the Latin American and Caribbean Addresses Registry (LACNIC) staff for many years and continues to collaborate with them on educational initiatives.

At a LACNIC meeting last March, senior network engineer José Domínguez gave tutorials on IPv6 and multicast. LACNIC's next meeting is scheduled for October 2004 in Costa Rica, where José will again be a presenter.

Acknowledgements. In addition to NSF grant funding, support for these recent NSRC activities has been provided by the Organization of American States, Cisco Systems, the Internet Society, Fundación para la Ciencia y la Tecnología, the International Development Research Centre, the Public Internet Registry, Qualys, O'Reilly Books, Cisco Press, Pearson Education, and DHL.

A brief history of the NSRC. The roots of the NSRC project trace back to a volunteer effort by Randy Bush to support networking in southern Africa in 1988, when he helped design and deploy a multi-country network that resulted in the first connections to the Internet for South Africa, Botswana, Namibia, Zimbabwe, and later, many others. The NSRC was formalized in 1992 by Randy Bush and John Klensin with a grant from the National Science Foundation, the first of several NSF grants to support NSRC activities.

For more information about the NSRC project, contact Steven Huter (sghuter@nsrc.org).

References

1. AfNOG:
<http://www.afnog.org/>
<http://ws.afnog.org/>
2. AfrinIC
<http://www.afrinic.net/sponsors.htm>
3. CEDIA Consortium:
<http://www.cedia.edu.ec/>
4. Internet Society (ISOC)
<http://www.isoc.org/>
<http://ws.edu.isoc.org/>
5. LACNIC:
<http://lacnic.net/sp/presentationsVI.html>
6. NSF:
<http://www.nsf.gov/>
7. NSRC:
<http://nsrc.org/>
8. Réseaux IP Européens Network Coordination Centre (RIPE NCC):
<http://ripe.net/>
9. SANOG:
<http://www.sanog.org/sanog4/>
10. Silk project:
<http://www.silkproject.org/>
11. WALC:
<http://www.walc03.ula.ve/>
<http://www.walc03.ula.ve/talleres/taller4.htm>

Organized Crime Invades Cyberspace

“The global criminal world of oil, narcotics and guns now has broadband.” This is how science fiction writer Bruce Sterling summed up the current Internet crime wave at a recent session of Gartner’s 10th annual IT Security Summit in Washington, D.C. Sterling contends that the solution is not more laws, but more aggressive prosecution of existing laws. For more details, see <http://www.internetnews.com/bus-news/article.php/3365491>

Credit Card Scam Catches Unsuspecting Consumers in a Web of ‘Triangulation’

In recent months, some people making purchases from online auction sites such as eBay have unwittingly been buying stolen merchandise in a type of scam known as “triangulation.”

In this type of fraud, criminals use stolen credit cards to buy merchandise from online retailers (usually small, specialized e-commerce sites that sell tools and appliances), then resell the goods at bargain prices on eBay. The unwitting buyers agree to pay with money orders or electronic fund transfers, allowing the thieves to easily convert their stolen credit card numbers into cash.

The Merchant Risk Council urges consumers to protect themselves by asking the seller to provide a product’s serial numbers before agreeing to purchase it. For more details, see <http://www.msnbc.msn.com/id/5158208>

Where Bank Card Fraud Thrives...

According to a crime research study, nearly half of the crimes related to bank card fraud are perpetrated by citizens of the former Yugoslavia, Romania, Nigeria, Pakistan, and Indonesia, while Americans commit only 1.7% of these crimes. For details, see <http://www.crime-research.org/news/13.04.2004/204>

Nigeria Continues Crackdown on Email Fraud

At the end of June, a Nigerian law enforcement agency reported it had detained over 500 email fraud suspects and seized more than \$500 million in ill-gotten gains. Nigeria also reported plans to deploy software that can aid in the fight against email fraud by identifying key words that typically appear in scammers’ emails. For details, see <http://business.iafrica.com/news/331660.htm>

Tough Sentence Sticks for Net Fraud

A con artist who posed as a licensed physician and charged for prescribing drugs over the Internet got no mercy from a federal appeals court when he sought to shorten his 77-month sentence. For details, see http://zdnet.com.com/2110-1104_2-5195986.html

Crooks Do Brisk Business Selling Access to Infected PCs

Virus writers are now peddling the IP addresses of infected machines (“BotNets”) in a burgeoning racket that’s attracted organized crime. This illegal trade is making spam investigations more difficult. See http://www.theregister.co.uk/2004/04/30/spam_biz/

“Turning the Tables on Email Swindlers”

A *New York Times* essay by Seth Schiesel describes how fraud baiters are waging a vigilante campaign to beat Internet scammers at their own game. For details, see <http://www.nytimes.com/2004/06/17/technology/circuits/17hoax.html?ex=1088511300&ei=1&en=26c910fd3660922a>

Other scam fighters have turned to humiliation as their weapon of choice, conning spammers into revealing themselves:

http://www.419eater.com/html/trophy_room.htm

New Weapons in the War Against Spam

Some spam fighters have gone undercover to wage war against spam. In a bid to glean vital insider information that could aid their mission, spam busters have begun infiltrating exclusive online spammer forums such as the Pro Bulk Club and bulkmails.org, which are normally open only to members with a proven track record in spamming. For details, see http://www.theregister.com//2004/05/14/spam_club/

Con Scheme Hijacks Phone Service for the Deaf

Internet callers from Nigeria and elsewhere recently hijacked a telephone relay system for deaf people in order to perpetrate their fraudulent schemes. For details, see <http://www.dailystar.com/dailystar/dailystar/17393.php>

FTC Settles with ‘Married but Lonely’ Spammers

According to the terms of an FTC settlement in May, Brian Westby and Martijn P. Bevelander, who are charged with using deceptive spam to trick recipients into visiting adult websites, were fined \$112,500 and barred from using false subject lines and false header information in email. For more details, see <http://www.ftc.gov/opa/2004/05/westbysettlement.htm>

Senate Moves to Criminalize Phishing

Up to five years of jail time plus hefty fines could be facing con artists who “phish” for users’ sensitive information on the Internet in ID theft schemes. For details, see “Senator introduces ‘phishing’ penalties bill” <http://computerworld.com/governmenttopics/government/legislation/story/0,10801,94490,00.html>

Five Essential Steps for Protecting Your PC



What's the absolute minimum you need to do to avoid viral infection these days? A *lot* more than you may think...

Dan Albrich

Manager, Microcomputer Services
dalbrich@uoregon.edu

There was a time when many Windows users felt comfortable with simply having an antivirus product with up-to-date definitions. While security experts would recommend a more complete regimen of actions to secure a Windows PC, it has not been common practice to do more.

However, the escalating onslaught of viruses in recent years—including those that infect a Windows PC simply when you connect to the network—has forever changed the minimal set of things you must do to keep your PC free from infection.

Although PC security is a moving target, here is what we would say is the *absolute minimum* set of things Windows users must do to avoid infection (presuming you connect to the Internet via dial-up modem or ethernet):

- 1. Enable the automatic update function built in to Windows 2000 and XP.** This setting can be found under the system control panel. Note that this automatic update function sometimes fails, so to be on the safe side we recommend manually running Windows Update *and* Office Update on a weekly basis. Note that running these updates is relatively fast and easy for ethernet-connected users, but much more time consuming for modem users.
- 2. Install antivirus software—and more importantly—keep it up-to-date!** Norton AntiVirus versions 2002 and newer do generally try to automatically update your virus definitions. When you open the application, you'll see your virus definition date displayed on the main status screen. Try not to let your virus definitions get more than a week old. You can update them by clicking on the "LiveUpdate" button when you are connected to the Internet.
- 3. Install Mozilla (an alternate web browser) and use it instead of Microsoft's Internet Explorer whenever possible.** See <http://www.mozilla.org/> to download the latest released version.

Note that you can safely install more than one web browser, and we are not suggesting that you delete Internet Explorer (IE). In fact, the Windows Update

mechanism and some websites essentially *require* IE's use. We're simply asking you to use an alternate browser like Mozilla for your general purpose needs, reserving IE's use for cases where you actually require it. This is primarily due to the large number of security vulnerabilities found in IE, many of which have not been patched at this time (for the latest on IE vulnerabilities, see the "Security Alerts" sections on pp. 12 and 15).

- 4. Install SpyBot.** Spybot is a freeware anti-spyware tool. Update its definitions (called *includes*) and scan for spyware on a regular basis. SpyBot is included on both the Duckware 2003 and UO Security CDs. You can also download the latest version at <http://www.safer-networking.org/> This tool will help make you aware of any spyware that is installed on your system.

You may also wish to look at another excellent program called Ad-aware (<http://www.lavasoftusa.com/>). Note, however, that Ad-aware is not free for educational use.

- 5. Avoid risky computing activities, such as surfing websites for copyrighted material or using peer-to-peer applications to download illicit material.** Aside from the obvious copyright considerations, also note that the content on these sites may include viruses which have been renamed as a ploy to trick you into opening them.



Lane County Makes Recycling E-waste Easier...

Thanks to a new program initiated by Lane County Solid Waste Recycling, you no longer have to wait for special recycling events in order to safely dispose of your outmoded electronic gear. E-waste is now accepted on a weekly basis.

Call **682-3111**, between 8 A.M. and 5 P.M., Monday through Friday to set up an appointment. For more information on the new recycling program, see

[http://www.lanecounty.org/
PW_WMD_Recycle/ewaste.htm](http://www.lanecounty.org/PW_WMD_Recycle/ewaste.htm)

Security Alerts...

— Microsoft Windows —

Proof of Concept Exploit Code for IE Vulnerability in Circulation

All versions of Microsoft Internet Explorer are vulnerable to an exploit that could allow an attacker to execute malicious code once a victim is tricked into viewing an HTML document (either a web page or HTML email). This exploit code is publicly available, and attacks have already been reported.

Users can reduce their risk by running Windows Update. To get more information and to download the cumulative update for Microsoft RPC/DCOM (828741), see MS Security Bulletin MS-012 at <http://www.microsoft.com/technet/security/bulletin/MS04-012.msp>

References:

1. US-CERT Vulnerability Note VU#713878:
<http://www.kb.cert.org/vuls/id/713878>
2. UK Government CERT Briefing Notice 286/04
<http://www.uniras.gov.uk/11/12/13/brief2004/brief-28604.txt>

Massive Security Hole in Eudora in Conjunction with IE (Windows)

In May, a major security flaw was discovered in the popular email client Eudora. The flaw specifically involves attachments opened in Microsoft Internet Explorer and affects all versions of Eudora. As of June 28, no patches have been released.

The main exploit can be avoided by *cutting and pasting URLs* that appear in Eudora email messages rather than clicking to open them. (This is good advice no matter what browser you use.) However, other security advisories suggest not using Eudora at all.

For those who continue using Eudora, Microcomputer Services has posted step-by-step instructions for turning off Eudora's vulnerable features at <http://micro.uoregon.edu/security/eudora/>

For details on Eudora's vulnerabilities, see

- "Eudora speared by massive security hole"
<http://www.techworld.com/security/news/index.cfm?NewsID=1516>
- "Secure Your PC...Do Not Use Eudora" at
<http://www.maths.usyd.edu.au:8000/u/psz/securepc.html#Eudoraxx>

MS04-011 Patch Critical

The MS04-011 patch is critical for Hosts Running Secure (via SSL) Services on Remotely Accessible NT/2K/XP/2003 Platforms. System administrators are urged to apply this patch, which fixes server vulnerabilities that could allow buffer overruns and remote code execution. Many of the security lists, including CERT, have reported that the exploit code for this vulnerability is in active use.

ActiveDirectory, Exchange Server, Internet Information Server (IIS), or any other software that utilizes the Microsoft SSL library are at risk. For details, see Microsoft Security Bulletin **MS04-11** at <http://www.microsoft.com/technet/security/bulletin/MS04-011.msp> and Knowledge Base Article KB835732 at <http://support.microsoft.com/default.aspx?scid=kb;en-us;835732>

Serious Security Flaw in RealOne Player, RealPlayer (Windows)

In June, RealNetworks Inc. acted to correct a critical security flaw that impacts millions of users of its popular RealOne Player and RealPlayer software. The flaw could potentially allow a hacker to execute malicious code on a targeted machine. The code runs in the security context of the logged-on user. Affected versions include:

- RealOne Player (English)
- RealOne Player 2 (all languages)
- RealPlayer 8 (all languages)
- Real Player 10 (English, German, and Japanese)
- RealPlayer Enterprise (all versions)

To update your Windows system, go to RealNetwork's Customer Support page at http://service.real.com/help/faq/security/040610_player/EN

For further details on the problem see SearchSecurity.com's article, "High severity flaw plagues RealOne Player, RealPlayer" at http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci969919,00.html

DirectPlay Vulnerability Could Allow Denial of Service Attacks

On June 8, Microsoft issued a "moderate" security warning for a DirectPlay vulnerability in Windows XP/98/98SE/Me and issued fixes for the problem. It's recommended that all Windows users consider applying the security update available on Microsoft's Security Bulletin **MS04-016** page at <http://www.microsoft.com/technet/security/bulletin/MS04-016.msp>

This page also contains a complete list of affected software and components.

W32.Gaobot.WX Worm Exploits Weak Passwords in Windows 2000/NT/XP

This worm spreads by exploiting multiple vulnerabilities, including weak passwords, to modify victims' files. It affects Windows 2000, NT, and XP systems. For details, current virus definitions, and removal instructions, see Symantec's Security Response page at <http://securityresponse.symantec.com/avcenter/venc/data/w32.gaobot.wx.html>

Also see Symantec's information on the W32.Gaobot.AUS worm (<http://securityresponse.symantec.com/avcenter/venc/data/w32.gaobot.aus.html>) and W32.Gaobot.SN worm (<http://securityresponse.symantec.com/avcenter/venc/data/w32.gaobot.sn.html>).

Windows Security CD Updates

Don't forget that current students, faculty, and staff are eligible to receive a free Windows Security CD, which contains vital antiviral updates and system patches specific to Windows machines. The CD is periodically updated to stay abreast of new security developments.

To obtain your copy of the CD, go to the Microcomputer Services Help Desk on the ground floor of McKenzie Hall (151 McKenzie) and present your UO ID to a consultant.

— Other Alerts —

TCP Vulnerabilities

If exploited, this vulnerability could allow a denial of service attack against existing TCP connections. You'll find a detailed explanation of the vulnerability, as well as available remedies, on the NISCC Vulnerability Advisory page at

<http://www.uniras.gov.uk/vuls/2004/236929/>

Flaw Discovered in Wi-Fi

A vulnerability in the 802.11 wireless standard could allow a relatively unsophisticated attacker to shut down networks within five seconds. Wide exploitation of this flaw is not expected. For details, see

http://www.theregister.co.uk/2004/05/13/wifi_security_flaw/

Three Symantec Firewall Flaws

Information on three vulnerabilities affecting several Symantec firewall products is available from US-CERT at the sites listed below. Users are advised to apply available patches:

<http://www.kb.cert.org/vuls/id/294998>

<http://www.kb.cert.org/vuls/id/682110>

<http://www.kb.cert.org/vuls/id/634414>

— Mac OS X —

Safari Web Browser Vulnerability

Latest Mac OS X software update includes the fix

If left unpatched, a security flaw in the Safari web browser could allow a remote user to execute malicious code over the network. Apple Security Update **2004-06-07** (available at <http://www.apple.com/support/downloads/>) fixes this and several other security holes for Mac OS 10.3.4 (Panther) and Mac OS 10.2.8 (Jaguar) systems and servers.

For details, see

- Secunia report
<http://secunia.com/advisories/11622/>
- US-CERT report
<http://www.kb.cert.org/vuls/id/210606>
- *The Register* ("Apple security patch problems fixed")
http://www.theregister.co.uk/2004/06/09/apple_security/

Easy way to stay current on Apple software downloads and patches: Mac OS X users can keep their systems up-to-date and patched more easily by setting up a frequent "Software Update" schedule in the System Preferences menu. "Software Update" checks for new software downloads and alerts you daily, weekly, or monthly, according to your preference.

To set this feature, open the Apple menu in the upper left corner of your screen and select "System Preferences." Click the "Update Software" button and check the box "Check for updates." Then select "daily," "weekly," or "monthly" from the "Check for updates" pull-down menu.

AS.MW2004.Trojan Targets Mac OS X

This virus masquerades as a Microsoft Word 2004 installer named "Microsoft Word 2004 OS X Web Install." Once activated, it attempts to delete a victim's home directory and its contents without warning.

For details and antivirus downloads, see Symantec's Security Response bulletin at

<http://securityresponse.symantec.com/avcenter/venc/data/macos.mw2004.trojan.html>

If you regularly run Norton Antivirus LiveUpdate, you should already have the latest antivirus definitions. To stay abreast of late-breaking viruses, see Symantec's comprehensive list of the latest virus threats at

<http://securityresponse.symantec.com/avcenter/vinfodb.html>

To Buy or Not to Buy: Renting versus

Joe St Sauver, Ph.D.

Director, User Services and Network Applications

joe@uoregon.edu

If you're interested in legally accessing music online, you face an interesting dilemma these days. On the one hand, you can buy music on a track-by-track basis from Apple's iTunes (or any of a number of other online music sellers, even including Walmart). After you've paid for a track, typically at \$0.99/track or less, you can listen to it forever.

On the other hand, you now also have the option of renting access to music for a flat monthly fee, for example from the now-legal Napster Premium service. Once you've signed up and for as long as you continue to pay a flat monthly fee, you get the ability to listen to virtually all the music that's been licensed and made available as "tethered downloads" (you can also buy favorite songs outright, as in the iTunes model).

The question that's obvious to any business major or cost-conscious consumer is, "Which model is the better deal for me?" As is typical for many questions of this sort, the answer is, "It depends."

Some time this summer, while you're waiting for the hamburgers to grill, dig out a piece of paper and a pencil and start making a list of *specific individual songs* that you and your family and friends really like. How long is that list? A hundred songs? Three hundred songs? A thousand songs? For the sake of argument, let's assume 300-350 songs or so. (That's how long my list was when I tried this exercise, but obviously everyone's list is going to be different, and I probably forgot some that I actually do like.)

Assume you could buy all those songs from iTunes for \$0.99/track (in reality, some of the songs may not be available, or you may already have copies of the music on CD). You now have an excellent initial estimate of what a pay-per-track service might cost—in our case, approximately \$300-\$350, assuming we never find any new songs we want to add to our collection in the future.

Now consider a music rental service like Napster. If it costs \$10/month to participate in a Napster-like music rental service, \$300 to \$350 will buy you roughly three years of music access. Which is better? Here's where the analysis gets tricky.

If I want 300-350 songs to listen to now, \$10/month lets me listen to all those songs today *if* I choose them from the rental model. If I want access to all of those 300-350 songs in the buy-a-track-at-a-time model right now, I'm looking at paying \$300-350 in front-loaded costs (ouch).

Moreover, I might like 300 or 350 songs *now*, but what if my musical tastes change? Instead of listening to classic rock, what if I develop a love of jazz, blues, classical, folk music, or country western? If that happens and I've chosen the buy-a-track-at-a-time route, my library of 300-350 favorite classic rock tracks (or whatever) becomes irrelevant, and I'll need to buy a whole new library of music to satisfy my evolving musical tastes. If, on the other hand, I'm renting music, I merely change the category of music I'm listening to, and soldier on. Renting obviously is more economical than buying music —*if* I have frequently changing musical tastes.

Or what about new music? I may have 300 or 350 favorites now, but hopefully I'll hear at least one or two new songs a month that I might want to add to my collection. If I'm buying music track-by-track, the meter will continue to tick every time I find a new favorite, while in the rental model, new music will be freely available to me. In fact, the more eclectic my musical tastes, and the larger the number of my current favorite songs, the better music rentals end up looking.

But depending on circumstances, the equation can tip the other way just as easily. For example, if you want to load tracks onto a portable device like an iPod or a portable MP3 player, you'll need to buy the tracks outright whether you're currently participating in a rental service or not. If you're routinely buying tracks on a track-by-track program, those costs are already covered; if you're renting music, however, the tracks you'll need to purchase in order to load them onto a portable device represent an additional cost of choosing the rental model rather than a straight track-by-track purchase model.

Evaluating the two models also forces me to do time-value financial forecasting: how many years might I rent music? Three years? Five years? Twenty years? The longer the rental period, the less appealing those ongoing rental programs look, particularly if I worry about per-month rental costs potentially increasing over time. But long time horizons also hurt track-by-track music purchasers: when you hit retirement age, are you *really* going to be listening to the same music you purchased twenty years ago? In some cases, sure; in other cases, maybe, maybe not.

In other cases, the format used to distribute music may be key. Apple's proprietary AAC encoding is closely tied to their iPod hardware, although they have iTunes clients for both Windows PCs and Macs. Napster, on the other hand, uses Microsoft's secure WMA format files, a format that is more broadly supported on a range of portable devices (but Napster has no Napster client for the Mac).

Either way, try compiling a list of favorite songs, and see how many favorites you end up with. It just might help you decide which online music model makes most sense for you.

Buying Music Online

Some Online Music Resources

1. iTunes: <http://www.apple.com/itunes/>
2. Napster: <http://www.napster.com/>
3. Walmart: <http://musicdownloads.walmart.com/>
4. Rhapsody (from Real): <http://www.listen.com/>
5. <http://www.buymusic.com/>
6. <http://www.connect.com/>
7. <http://www.emusic.com/>

8. <http://www.musicmatch.com/>
9. <http://www.musicnow.com/>
10. *PC World*: “Online Music: New Hits and Misses”
<http://www.pcworld.com/reviews/article/0,aid,111643,pg,1,00.asp>
11. *USA Today*: “Wired for sound: Music download services that rock”
http://www.usatoday.com/life/music/reviews/2004-04-12-legal-download-review_x.htm

Late-Breaking Security Alerts...

Mozilla Security Issue (Windows only)

To protect themselves from a recently discovered shell: protocol security issue, users of Mozilla, Firefox, and Thunderbird who run Windows should either update to the newest full release of each of these products or install a security patch released on July 8. To learn more about the issue and how to fix it, go to <http://www.mozilla.org/security/shell.html>

Test Your Browser for Frame Injection Vulnerability

Nearly a dozen browsers are vulnerable to a particular form of “spoofing” (faking) that can allow malicious content to be injected into a browser window that is owned by a trusted site. The following browsers are known to be vulnerable, and there may yet be more:

- Opera 7.51 for Windows
- Opera 7.50 for Linux
- Mozilla 1.6 for Windows and Linux
- Mozilla Firebird 0.7 for Linux
- Mozilla Firefox 0.8 for Windows
- Netscape 7.1 for Windows
- Internet Explorer 5.2.3 for Mac
- Safari 1.2.2
- Konqueror 3.1-15redhat

For more details, and to check your browser for this vulnerability using Secunia’s test, go to <http://secunia.com/advisories/11978/>

More IE Exploits

In July, Microsoft issued a stop-gap fix for one of many malicious exploits that have plagued Internet Explorer in recent months and prompted some security agencies (notably US-CERT) to recommend that users consider

switching to another browser altogether. This particular flaw, which is related to the ADODB.Stream object in the operating system’s Data Access Components, will be eradicated in Windows XP Service Pack 2, slated for release in August. For details, see

- “Microsoft Plugs IE...”:
<http://www.techweb.com/wire/story/TWB20040702S0007>
- Microsoft Knowledge Base Article KB870669:
<http://www.microsoft.com/downloads/details.aspx?FamilyID=4d056748-c538-46f6-b7c8-2fbfd0d237e3&displaylang=en>
- “U.S. Steers Consumers Away from IE”:
http://story.news.yahoo.com/news?tmpl=story&cid=74&e=3&u=/cmp/20040702/tc_cmp/22103407

CoolWebSearch Trojan Wreaks Havoc

This nasty, difficult-to-eradicate browser hijacker makes life miserable for Windows users in many ways. In addition to significantly slowing PC performance, CoolWebSearch can cause Windows to freeze, crash, or randomly reboot. It installs dozens of bookmarks to porn sites on your Windows desktop, adds a toolbar to Internet Explorer, and changes your home page without your consent. For more details on this malicious trojan, see “CoolWebSearch is winning Trojan war” at http://theregister.com/2004/06/29/cws_shredder/

NAV DoS Vulnerability

A security researcher recently reported a glitch in Norton AntiVirus (NAV) that under certain conditions can trigger a denial of service attack. The problem has been traced to the NAV file repair engine and occurs when NAV scans some specially crafted compressed files. For details, see the advisory at http://www.geocities.com/visitbipin/Nav_dos_part_3.html

Don't Be Fooled by Bogus Viral 'Scanned, No Virus Found' Messages

Users should be aware that viruses are now routinely including fake “This message has been scanned for viruses by <fill in well known antivirus product name here>; no viruses were found.” In fact, the messages *do* have a virus, notwithstanding their false claim to have been scanned and found virus-free. Our virus stripping/defanging should handle these viral messages just like all the other viruses we see, but if you read your email on some other system that doesn’t strip or defang viruses, don’t be taken in by the virus writer’s lies.

Getting Started with SAS's PROC MIXED: Analyzing



How PROC MIXED lets you make inferences about fixed effects that apply to entire populations of random effects

Robin High

Statistical Programmer and Consultant
robinh@uoregon.edu

For almost 30 years now, PROC GLM (General Linear Models) has been one of SAS's most important analysis routines. In addition to being able to analyze unbalanced designs, PROC GLM was designed to compute fixed effects analysis of variance and covariance models in a manner that combines features from both PROC ANOVA (analysis of variance) and PROC REG (regression). Its task is to fit a variety of linear models to experimental or observational data, enabling you to make statistical inferences.

But now a comparatively new procedure called PROC MIXED gives you even more power to analyze a wide variety of analysis of variance and covariance models with balanced or unbalanced datasets. (For a comparison of some of the features of PROC MIXED with PROC GLM, see <http://cc.uoregon.edu/cnews/summer2001/procmixed.html>)

To illustrate how the PROC MIXED procedure works, consider this example drawn from Chapter 41 of the *SAS/STAT User's Guide* (see **References** section at the end of this article), which uses SAS commands to read an unbalanced dataset of children's heights that was collected from four families in a specified region:

```
DATA heights;
INPUT family obs gender $ height @@;
CARDS;
1 1 F 67      1 2 F 66      1 3 F 64
1 1 M 71      1 2 M 72
2 1 F 63      2 2 F 63      2 3 F 67
2 1 M 69      2 2 M 68      2 3 M 70
3 1 F 63      3 1 M 64
4 1 F 67      4 2 F 66
4 1 M 67      4 2 M 67      4 3 M 69
;
PROC TABULATE NOseps;
CLASS family gender obs;
VAR height;
TABLE family, gender*obs=' ' *height='
'*sum=' '*f=6.0
/ rts=10 BOX=' Heights' misstext=' ' ;
RUN;
```

In this example, the response variable *height* measures the heights (in inches) of 18 individuals who are classified according to their respective family and gender. Results are shown in the following table:

HEIGHTS	GENDER					
	F			M		
	1	2	3	1	2	3
FAMILY						
1	67	66	64	71	72	
2	63	63	67	69	68	70
3	63			64		
4	67	66	67	67	69	

You can also perform a traditional two-way analysis of variance (ANOVA) of these unbalanced data (which produces output similar to what you get with PROC GLM) by using the following PROC MIXED statements:

```
PROC MIXED DATA=heights NOitprint;
CLASS gender family;
MODEL height = gender family family*gender;
RUN;
```

In this example, the PROC MIXED statement invokes the procedure and identifies the SAS dataset. The CLASS statement treats both family and gender as classification variables. For this analysis, both *gender* and *family* are treated as fixed effects (i.e., gender can only be male or female and these four families are the only levels of interest).

The MODEL statement specifies the continuous response (or dependent) variable, height, which is placed to the left of the equal sign. The explanatory (or independent) variables are listed to the right of the equal sign. In this example the two explanatory variables are categorical, as they represent levels of gender and family; they comprise the main effects of the design. The third term, FAMILY*GENDER, provides a way to test for the interaction between the two main effects.

PROC MIXED computes dummy variables associated with *gender*, *family*, and *family*gender* to construct the nxp design (X) matrix for the linear model. A column of 1's is also included as the first column of X to model the intercept. By the assumption of independence, the residual matrix, R, is equal to $\sigma^2 * \mathbf{I}_{18}$ where \mathbf{I}_{18} is an 18x18 identity matrix.

The RUN; statement completes the list of statements for this procedure. The coding looks very similar to PROC GLM statements. However, the output from PROC MIXED takes on a somewhat different look than that produced by PROC GLM:

Fixed Effects that Apply to Clustered Data

Class	Levels	Values
FAMILY	4	1 2 3 4
GENDER	2	F M

Table 1: Class Level Information

The “Class Level Information” in Table 1 lists the values of all classification variables specified in the CLASS statement. It also tells you the order SAS interprets levels of categorical variables. Check this table to make sure that the data have been coded and read in to the SAS dataset correctly.

Cov Parm	Estimate
Residual	2.10000000

Table 2: Covariance Parameter Estimates (REML)

The “Covariance Parameter Estimates” in Table 2 display the estimate of the residual variance, σ^2 , for the model (analogous to Mean Square Error from PROC GLM).

Source	NDF	DD	Type III F	Pr > F
GENDER	1	10	17.63	0.0018
FAMILY	3	10	5.90	0.0139
FAMILY*GENDER	3	10	2.89	0.0889

Table 3: Tests of Fixed Effects

Table 3 shows the Type III significance tests for the fixed effects listed in the MODEL statement. The Type III F-statistics and p-values are the same as those produced by the Type III analysis from PROC GLM. However, because PROC MIXED applies a likelihood-based estimation scheme by default, it does not compute or display sums of squares or mean squares.

The Type III test for the interaction effect, *family*gender*, is not significant at the 5% level, but the tests for both main effects are significant. As long as you don’t enter a RANDOM or REPEATED statement, the analyses from both PROC MIXED and PROC GLM will agree if the model contains only fixed effects.

The assumptions concerning the residuals from an analysis of variance include:

- normally distributed
- independent
- have constant variance

The normality assumption is probably realistic in this example since observed heights are measured on a reasonably continuous scale and the absolute lower limit of 0 is not even close to the smallest values observed. However, since the data were collected from clusters (families), it is very likely that the heights from members of the same family are positively correlated with each other (i.e., they should not be treated as independent observations).

The methods implemented in PROC MIXED are also based on the assumption of normally distributed data; however, the assumption of independence can be modified by modeling statistical correlation in a variety of ways. You can also work with heterogeneous variances, that is, variances that are not constant across the groups. I will examine these two features with the REPEATED statement in the fall issue of *Computing News*.

For the children’s height data, one of the simplest ways to model the correlation is through inclusion of a random effect. Since the four families were actually selected at random from a large population, the effect for family is assumed to be a random variable that is normally distributed with zero mean and some unknown variance, σ^2 . Declaring family as a random effect in this model sets up a common correlation among all heights measured from the same family.

The interaction of *family*gender* as a second random effect also accounts for the correlation between all observations that have the same level of both family and gender. One interpretation is that females will have a higher (or lower) correlation with other females in the same family than males will have with other males in the same family. With the height data, this random effects model seems reasonable. Here is the code to fit this mixed model (which includes both random and fixed effects) in PROC MIXED:

```
PROC MIXED DATA=heights NOitprint;
CLASS gender family;
MODEL height = gender;
RANDOM family family*gender / subject=family type=vc
vcorr ;
RUN;
```

The random effects, *family* and *family*gender*, are now listed only on the RANDOM statement (notice the two terms must not appear on the MODEL statement with PROC MIXED). The **type=vc** option specifies the variance components model for both *family* and *family*gender*. The residual matrix is assumed to equal $\sigma^2 \mathbf{I}_{18}$, where \mathbf{I} is an 18×18 identity matrix. The output from this revised analysis is as follows.

Row	Col1	Col2	Col3	Col4	Col5
1	1.000	0.658	0.658	0.379	0.378
2	0.658	1.000	0.658	0.379	0.378
3	0.658	0.658	1.000	0.379	0.378
4	0.379	0.379	0.379	1.000	0.658
5	0.379	0.379	0.379	0.658	1.000

Table 4: Estimated V Correlation Matrix for Family 1

Table 4 shows the computed correlation matrix for family 1. These data were given in row 1 of the data table, which has 5 members (3 females and 2 males). Columns

PROC MIXED, continued...

1-3 and rows 1-3, along with columns 4-5 and rows 4-5, show the correlations of females with females and males with males is 0.658. The remaining cells indicate the correlation among the females and males within the family is 0.379.

Cov Parm	Estimate
FAMILY	2.4010
FAMILY*GENDER	1.7657
RESIDUAL	2.1668

Table 5: Covariance Parameter Estimates (REML)

Table 5 displays the results of the REML fit. The “Estimate” column contains the variance component estimates for FAMILY and FAMILY*GENDER, as well as the residual variance, $\sigma^2=2.1668$. PROC MIXED and PROC GLM estimate variance components from the linear model with different methods. PROC GLM uses method-of-moments estimators while PROC MIXED uses several options, including moment estimates (with METHOD=typen where $n=1, 2,$ or 3) maximum likelihood (METHOD=ml) or restricted/residual maximum likelihood (METHOD=reml), the default. The type of estimation method you choose may lead to different answers, especially with random effects or unbalanced data.

Source	NDF	DDF	Type III	F	Pr > F
GENDER	1	3		7.95	0.0667

Table 6: Type 3 Tests of Fixed Effects

Table 6 contains the significance test for the fixed effect, GENDER. Note that its p-value ($p=0.0667$) is larger than the one observed in the first statistical model that assumed all fixed effects ($p=0.0139$). The contrast in these two results illustrates the importance of modeling family as a random, rather than a fixed, effect. In fact, if 0.05 is applied as the cutoff point for significance, the fixed effects model shows a significant effect, whereas the model with random effects does not.

An additional benefit of a random effects analysis is that it enables you to make inferences about gender that apply to a population of families, whereas the inferences about gender from the analysis where *family* and *family*gender* are treated as fixed effects apply only to the particular families present in the dataset.

This simple example was designed to show you how PROC MIXED lets you model correlation in your data directly and make inferences about fixed effects that apply to entire populations of random effects.

References

1. Littell, R.C., Milliken, G.A., Stroup, W.W., and Wolfinger, R.D. (1996). *SAS System for Mixed Models*, SAS Institute, Cary, NC.
2. *SAS/STAT User's Guide: The Mixed Procedure*. Chapter 41, Section 6 “Clustered Data Example,” <http://www.id.unizh.ch/software/unix/statmath/sas/sasdoc/stat/chap41/sect6.htm> and <http://sas.uoregon.edu/sashtml/stat/chap41/sect6.htm>

NFSv4 and NFS Security

Joe St Sauver, Ph.D.

Director, User Services and Network Applications
joe@uoregon.edu

If you use NFS (Network File System) to share file systems between multiple computers, you are probably using NFS Version 2 or 3. However, you should know that NFSv4 is under active development and is available for trial use under a variety of operating systems.

NFSv4 offers numerous advantages over NFSv2 and NFSv3, including dealing with a variety of security issues mentioned in RFC2623 (“NFS Version 2 and Version 3 Security Issues and the NFS Protocol’s Use of RPCSEC_GSS and Kerberos V5,” <http://www.ietf.org/rfc/rfc2623.txt>).

Those of you currently running NFS v2 or NFS v3 may also be interested in the other NFS security references mentioned below.

References

1. NFS Version 4: <http://nfsv4.org/>
2. Network Appliance—The NFS Version 4 Protocol (nice introduction): http://www.netapp.com/tech_library/3085.html
3. CITI Projects: NFS Version 4 Open Source Reference Implementation: <http://www.citi.umich.edu/projects/nfsv4/>
4. Learning NFSv4 With Fedora Core 2: <http://www.vanemery.com/Linux/NFSv4/NFSv4-no-rpcsec.html>
5. CERT Advisory CA-1994-15 NFS Vulnerabilities: <http://www.cert.org/advisories/CA-1994-15.html>
6. NFS Security: http://www.linuxsecurity.com/feature_stories/feature_story-118.html
7. Security and NFS: <http://nfs.sourceforge.net/nfs-howto/security.html>
8. Secure NFS and NIS via SSH Tunnel: <http://www.math.ualberta.ca/imaging/snfs/>

Some Things You Need to Know about Spyware...



How to keep your Windows network connection humming after removing spyware

Spencer Smith

Microcomputer Support Specialist
spencera@uoregon.edu

Spyware and adware are becoming a huge problem for everyone who connects to the Internet.

In case you didn't already know, Spyware is a program that reports information about you and your Internet usage back to a central server, and adware are programs that cause the pesky pop-up windows to blare advertisements randomly every time you connect to the network. These programs can slow your computer to a crawl, and often redirect all your web browsing activity through their own servers to observe and catalog your Internet activity.

The load of spyware and adware grows the longer you browse the Internet; the current largest number of individual spyware components found on one machine brought to Microcomputer Services was 2100 items! This load of advertisements and background activity can take a fast computer and slow it to a complete stop. If you've noticed a lot of pop-up advertising while you surf the 'net and your computer has begun to crawl like molasses in January, you may be infested with Spyware.

There are several tools available to delouse your computer of its accumulated spyware and adware. Spybot (<http://www.safer-networking.org/>) and Ad-aware (<http://www.lavasoftusa.com/support/download/>) can scan for and eliminate these unwanted programs. However, eliminating the spyware can have other unwanted side-effects.

Some spyware modifies the Windows operating system, changing the way the TCP/IP connection is routed at a very low level. Removing the spyware can leave your Internet connection subtly broken; often it can send out information (good for the spyware people), but not receive information (bad for you).

The major symptom of this network stack corruption is the lack of a valid TCP/IP address. The WinSock2 stack can become so broken that it is unable to accept and decipher the information from the local network.

When this happens, Windows gives up and assigns itself an address that looks like '169.xx.xx.xx', where 'xx' is some random number between 0 and 255. If you examine your IP address and it has '169' as its first parameter, your WinSock2 stack may be corrupted.

This default address can also indicate a lack of signal from your Ethernet connection. If you are on campus or connected to the campus network, this lack of address could also indicate that your network jack has been disabled due to a worm or virus infestation. Unless you've just scanned for and eliminated spyware on your computer, you should investigate the Ethernet cable, your network jack, and your Internet connection by calling ResNet (346-4223) for problems in the residence halls, or Network Services (346-4395) for all other Ethernet connections. They will be able to tell you if your Ethernet connection has been disabled, and why.

WinSock2 Fix: There is a tool available online that will fix this Registry/protocol corruption, and restore your Internet connectivity. If you can get to an uncorrupted computer, the WinSock2 fix (for Windows 98, ME and 2000) is available at
<ftp://public.uoregon.edu/software/Utilities/WinsockFix.exe>

For Windows XP, the URL is
<ftp://public.uoregon.edu/software/Utilities/WinsockXPFix.exe>

The tool is also included on the **UO Security CD**, available in Room 151 McKenzie Hall. *Be sure to get the most current version of this CD*; the problems, worms, and viruses it detects and disinfects changes constantly, and new revisions of the CD are being created frequently.

WinSock2 is a freeware tool written by Theron Skryba of Option Explicit Software. It comes with no warranty of any kind, but has appeared to work very well in all the trials we've given it here at Microcomputer Services.

Scanning for and eliminating unwanted spyware and adware programs should be a part of your ongoing, standard maintenance. Scan your computer at least once a week for spyware and adware. Scan for viruses at the same time; a weekly scan is recommended. Update your virus definitions and spyware definitions frequently. Norton AntiVirus, Spybot, and Ad-aware all have online updates integrated into their scanning programs.

If you have any questions about your Internet connectivity, or would like some help checking on your account's status, feel free to call Microcomputer Services at **346-4412**. You can also reach us via email at microhelp@lists.uoregon.edu.

Computing Without Using Your Mouse:

Joe St Sauver, Ph.D.

Director, User Services and Network Applications
joe@uoregon.edu

A common misconception is that everything that's on the Internet is on the World Wide Web. Others believe that if you want to use the Internet, you must click on things in a graphical user environment (such as Internet Explorer running under Windows).

Well, that's just not the case. There's a whole other world out there, just waiting for you to discover it, if you don't mind typing a little—it's the world of the Unix percent sign, or shell prompt. The shell prompt isn't for everyone, and if you're happy using what you've got you don't need to try it out. If you *do* try it, though, you may find you actually like it.

The following brief overview of Unix-speak is not meant to make you a shell prompt expert, it is just meant to alert you to some possibilities you may not otherwise be aware of.

Getting to the Shell Prompt

If you're a UO user, you should have an account on Darkwing (if you're a faculty member/staff person/grad student), or Gladstone (if you're an undergraduate student). This is the account you likely use for email, to dial in to the UO's modem pool, for wireless access, or for access to UO VPN or Blackboard.

To login to that Darkwing or Gladstone account, use ssh (secure shell):

- **Windows PC:** On a PC running Windows, first make sure you've installed SSH Secure Shell from the PC Duckware CD-ROM, then see <http://micro.uoregon.edu/security/ssh/shell.html>

- **Macintosh:** SSH is provided as part of Mac OS X. To use the integrated secure shell client to login to Darkwing or Gladstone, begin by opening a terminal window on your Mac, then enter either:

```
ssh -l yourusername darkwing.uoregon.edu  
or  
ssh -l yourusername gladstone.uoregon.edu
```

If this is the first time you're using SSH to connect, you will need to agree to accept the cryptographic credential associated with Darkwing or Gladstone. After that, you'll be prompted to enter the password for your account.

When you connect, you'll be working in a terminal window that emulates (or imitates) a Digital Equipment

VT100-compatible terminal. (In the old days, before the advent of PCs, we old-timers actually used real VT100 terminals.)

Okay, I See a % Sign, Now What?

Once you see the percent sign prompt, you're ready to enter a Unix shell command. There are no menus and there's nothing to click on—you just need to know what commands to type.

One command that every user needs to know is **logout** (to logout from the shell prompt). Be sure to remember to *always* logout when you're done working at the shell prompt!

All Unix commands are case sensitive, and most Unix commands will be lowercase, rather short, and may not appear to be very adroitly named.

For example, to see documentation ("manual pages") describing Unix commands, you'd enter the **man** command at the percent sign prompt:

```
% man
```

But if you try that, don't be disappointed when all you see is:

```
usage: man [-] [-adFlrt] [-M path] [-T macro-  
package ] [ -s section ] name ...  
man [-M path] -k keyword ...  
man [-M path] -f file ...
```

If you're determined to learn more about the **man** command, try:

```
% man man
```

Again, you may be disappointed. **Man** pages are written in a very stylized way and are not particularly "user-friendly."

In general, you'll be better off trying one of the Unix books available from the Computing Center Documents Room, such as Harley Hahn's *A Student Guide to Unix*, or you can start with the very brief summary of common Unix commands at <http://cc.uoregon.edu/basicunix.html>

Editing Files

Before the advent of Microsoft Word, people created and edited text files using a "text editor" such as *vi*, *emacs*, or *pico*. Darkwing and Gladstone use two different such text editors by default:

- On Darkwing, the default editor is *vi*, as described at <http://cc.uoregon.edu/usingvi.html>
- On Gladstone, the default editor is *pico*, a simpler, menu-driven editor.

Rediscovering the Shell Prompt

Reading Email Without Using Web Email, Eudora, or Outlook

You may be surprised to learn that you can read your email online at the percent sign prompt without using web email, Eudora, or Outlook. To do this, at the percent sign prompt simply enter **pine**:

```
% pine
```

The *pine* email program is menu driven, like the *pico* editor that Gladstone uses. (For more details on pine, see the handout “Using Pine for E-Mail” at <http://cc.uoregon.edu/acrobatdocs/pine.pdf>)

Looking at Web Pages From the Command Line

You can also look at web pages without using Internet Explorer, Mozilla, or some other graphical web browser. At the percent sign prompt, enter:

```
% lynx http://www.google.com/
```

to go to Google. You can move around using your arrow keys and search for a topic (such as “hockey”) by typing it on the dotted line, then hitting the down arrow to “Google Search” and pressing return.

“Why Would I Want To Do This?”

At this point, you may be wondering, “Why on earth would I *want* to do stuff at the percent sign prompt?”

Working at the percent sign prompt is much like driving a car with a stick shift. Yes, driving a stick shift can be harder than driving an automatic transmission, but the stick shift may give you better control, or be cheaper, or may be the only option for specialized vehicles (such as large trucks), or driving a stick shift may just simply be more fun.

Working at the shell prompt can be much the same way: it can be quite efficient once you get the hang of it, and many people even find it rather satisfying. Using *pine* at the shell prompt largely eliminates the risk of getting a virus or worm in email, and using a command-line web browser (such as *lynx*) can make you sensitive to the issues that the visually impaired encounter when using a screen reader to access web pages.

We’d encourage you to get a good Unix book from the Documents Room (175 McKenzie Hall) and give it a try!

New Books on Security in Docs Room: Get Tips from the Pros

Vickie Nelson
Documents Room Librarian
vmn@uoregon.edu

Want to get up to speed on computer security? Below we’ve listed some of the latest books on this topic acquired by the Computing Center Documents Room (175 McKenzie Hall). The Docs Room is open 9:30 A.M. to 5 P.M. Monday through Friday.

Exploiting Software: How to Break Code. Greg Hoglund. Addison-Wesley, 2004.

Hoglund describes the attack strategies most commonly used to search for holes in your software and exploit them. Find out how to fix what’s wrong now, and learn ways to avoid future problems.

Hardening windows. Jonathan Hassell. Apress, 2004.

Hassell presents a quick checklist-style reference of 145 suggestions to help system administrators harden Windows NT, 2000, XP, or Server 2003, and includes tips on the endless task of patch management.

Network Security Assessment. Chris McNab. O’Reilly, 2004. Former

hacker Chris McNab shows network administrators how to search for vulnerabilities in their networks just the way a determined intruder would.

Security Warrior. Cyrus Peikari and Anton Chuvakin. O’Reilly, 2004.

The words “Know your Enemy” float over the title of this in-depth book on security, which is divided into four major sections: *Software Cracking* (including reverse engineering), *Network Stalking*, *Platform Attacks*, and *Advanced Defense*.

The Shellcoder’s Handbook. Jack Koziol, David Litchfield, Dave Aitel, and others. Wiley, 2004.

Several contributors to BugTraq, the vulnerability tracking mailing list, share knowledge and insights to improve your penetration testing skills and help you find—and close—security holes.

Stealing the Network: How to Own the Box. Ryan Russell. Syngress, 2003.

Russell uses first-person stories that focus on various kinds of network attacks to give readers a sense of how intruders think, what software and methods they use, and techniques of tracking and repelling them.

Geographical Limits of UO's Wireless Internet Service

Joe St Sauver, Ph.D.

Director, User Services and Network Applications
joe@uoregon.edu

As 802.11b/a/g wireless networking (WiFi) becomes more ubiquitous on campus, some users have mistakenly come to expect that the UO's wireless Internet service will also be available throughout the Eugene/Springfield metro area. Unfortunately, the UO's wireless Internet access is available only in the areas shown in the wireless map of campus (see <http://micro.uoregon.edu/wireless/>).

If you are "just barely" off campus, you may see "signal leakage" from a UO wireless access point located nearby. However, you should not expect to routinely receive reliable UO wireless service at any off-campus location. Moreover, even if you are able to connect to a network off campus that claims to be "uowireless," you should not assume it is the *real* UO wireless network; it may very well be a misconfigured private access point or someone masquerading as a genuine UO wireless access point in order to capture your network traffic.

Because you authenticate to the UO wireless network by providing your email address and password, you should be sure that you provide those credentials *only* to the secure web page at

<https://uowireless.uoregon.edu/>

Even then, you should make sure the SSL certificate for that host is valid before providing your information.

Whenever you use the wireless network, you should also always protect your wireless traffic from being overheard by eavesdroppers. One way to do that is by using the UO's Virtual Private Network (VPN), as described at <http://cc.uoregon.edu/cnews/spring2002/vpn.html>

If you have any questions about the UO's VPN service, see http://micro.uoregon.edu/getconnected/vpn_overview.html

« sites worth seeing »

- 1. Campus Energy Project and UO Virtual Energy Tour...**
Detailed information about campus energy use and conservation effort, including a links to a "Virtual Energy Tour" and a video produced by students from the Environmental Studies Service Learning Program:
<http://www.uoregon.edu/~ecostudy/slp/energy/>
- 2. "Anti-Phishing Working Group"...** The latest news and statistics on recent phishing attacks, with advice on how to protect yourself:
<http://www.antiphishing.org/>
- 3. The Federal Trade Commision's final ruling on email containing sexually oriented material...** The full text of the FTC ruling, which was issued on April 19:
<http://www.ftc.gov/os/2004/04/040413adultemailfinalrule.pdf>
- 4. ARTstor...** The Andrew W. Mellon Foundation's online test site, which archives images and art data for educational and scholarly use. The UO is one of 14 colleges, campuses, and museums invited to test the site and offer suggestions:
<http://test.artstor.org/>
- 5. "Turning the Pages"...** An interactive site featuring digitized versions of rare manuscripts:
<http://www.bl.uk/collections/treasures/digitisation1.html>
- 6. Classical Music Library...** Another web test site designed for libraries and educators. The interactive site provides access to a growing list of high quality recordings:
<http://orbis.classical.com/>
- 7. Netfilter/iptables project (Linux 2.4x and 2.6x)...**
Information about building Internet firewalls based on both stateless and stateful packet filtering, implementing NAT, manipulating packets, and more:
<http://www.netfilter.org/>
- 8. "Check List for members using @oregon addresses"...**
If you own one or two campus mailing lists and need to find subscribers who haven't yet migrated to Darkwing, use the interactive form at
<http://darkwing.uoregon.edu/cgi-bin/majordomo/tools/or.cgi>
- 9. "The Little Engine that Could"...** Robert Cringely's entertaining essay on the Linksys WRT₅₄G, a wireless access point and router that promises to change the world as we know it:
<http://www.pbs.org/cringely/pulpit/pulpit20040527.html>
- 10. "Brian's Buzz on Windows"...** The latest on Windows from Brian Livingston, including security insights, book reviews, and power user tips:
<http://briansbuzz.com/w/040506/>

Computer Conundrums Got You Down?



Try these tips for making troubleshooting less painful

Patrick Chinn

Distributed Network Computing Consultant
pchinn@uoregon.edu

Six Steps to Getting Good Technical Support

When your computer fails to cooperate, do you hesitate to call for technical support?

Solving problems over the telephone can sometimes be a challenge for both the caller and support personnel. Here are six steps to make those calls less painful and more productive.

1. Write Down the Error Message

The error message may not sound useful but it may be the critical piece required to solve your problem. When you get an error message, write it down and have that information available when you call.

2. Try Reproducing the Problem

Some problems are transitory. Discovering what steps cause the error often helps define the problem more clearly. When you encounter a problem, stop and think about what process you followed to get there. Write it down and try those steps again. If the problem persists, call technical support and let them know what procedure is producing the problem.

3. Be at the Computer

Solving a problem often involves checking program settings or working through a trial-and-error process. If you call from the computer we can be much more effective in solving the problem.

4. Gather Pertinent Information

Before calling for technical support, make a list of the following:

- Your computer model, if the problem is hardware-related
- What operating system you are using
- The name and version of the program that is having the problem
- Your email address, if the problem is email-related

5. Be Patient

Those of us answering the phone cannot see your computer, so we need to ask questions and to use you as our eyes. In some cases we may know the solution immediately. Please be patient while we investigate the problem and work to find a solution. If your time is limited, please find another opportunity to call.

6. Be Polite

Computer problems can certainly make a person angry, but yelling and using profanity will get you no closer to solving the problem. Take a deep breath and count to ten before picking up the phone. If you feel angry or frustrated by the support call, politely but firmly ask to speak with a supervisor.

Quick Tricks to Solving Your Own Problem

Restart

If a software program is failing, try quitting the program and restarting it. If the problem seems to be the computer's operating system or Internet connection, try restarting the computer. Many printer problems are quickly fixed by turning off the printer, waiting five seconds, then turning it back on.

Google the Error Message

This is the ultimate technical support trick. Have Google search for the error message. If the error

is common, Google will return numerous web pages with solutions to the problem.

Conversely, if Google returns only a few links, then the error message is either too specific or the problem is very rare.

Check the Manufacturer's Website

Many companies have made much of their tech support material available online. Use Google to find the manufacturer's website and check the support section for solutions. Look in areas called FAQs (Frequently Asked Questions) and Knowledge Bases. (*Hint: If you haven't found the answer within 15 minutes, you will most likely not find the answer at all.*)

Simplify

Think back to when the problem started to occur. Did you install new hardware or software? If so, try removing that component or program and see if the problem disappears.

Take a Step Back

Computers and software are tools. Often there are several different ways to accomplish the same task. If one process is failing, take a step back and ask yourself if there is another way to accomplish the same (or similar) goal. Sometimes the fastest solution to a problem is to bypass it entirely.

Check the Manual or Online Help

A printed manual, book, or online help usually won't help you solve a problem. However, they are invaluable resources whenever you find yourself asking, "How do I...?" Don't cheat yourself of an opportunity to find a quick answer to such questions as "What is ColorSync?", "How do I turn hyphenation on and off?", "How do I set up my printer?", or "What's the keyboard shortcut for...?" Most often, you can find the answers to these and similar questions in the documentation.

COMPUTING CENTER GUIDE

UO Website

<http://www.uoregon.edu/>

Computing Center Website

<http://cc.uoregon.edu/>

Microcomputer Services

<http://micro.uoregon.edu/>

(151 McKenzie Hall)

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

346-4412

microhelp@lists.uoregon.edu

Documents Room Library

<http://darkwing.uoregon.edu/~docsrn/>
(175 McKenzie Hall)

346-4406

Modem Number

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

Large Systems Consulting

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

(225-239 Computing Center)

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

346-1758

consult@darkwing.uoregon.edu

consult@gladstone.uoregon.edu

consult@oregon.uoregon.edu

Statistics Consulting

Robin High

219 Computing Center

346-1718

robinh@uoregon.edu

Electronics Shop (151 McKenzie Hall)

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

Computer hardware repair, installation, and upgrades.

346-3548

hardwarehelp@oregon.uoregon.edu

Network Services

<http://ns.uoregon.edu/>

Provides central data communication and networking services to the UO community.

346-4395

nethelp@oregon.uoregon.edu

Administrative Services

<http://ccadmin.uoregon.edu/>

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

Computing Center Hours

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

McKenzie Building Hours

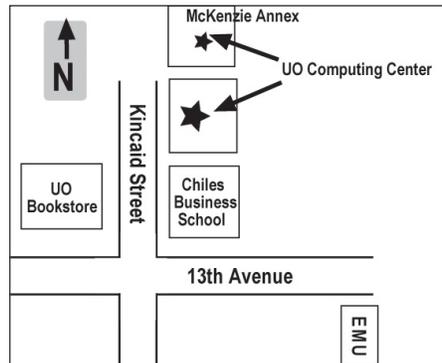
Mon - Thu 7:30 A.M. - 11:30 P.M.

Friday 7:30 A.M. - 7:30 P.M.

Saturday 9 A.M. - 9:30 P.M.

Sunday 9 A.M. - 8:30 P.M.

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



UNIVERSITY OF OREGON

UO COMPUTING CENTER

1212 University of Oregon Eugene, OR 97403-1212