Information Technology News of the University of California, Davis

IT TIMES

March 1999

http://it.ucdavis.edu/it.times/

In This Issue

Banner Upgrade 3

Configuring Eudora Pro 4.0
To Access Campus Modem Pools 4

Emergency Network
Security Policy 1

Site Licensing News 2

UCDNet2 Will Extend
Campus Network 2

Emergency Network Security Policy Issued to Protect Campus Resources

On February 12, the Office of the Chancellor issued Directive #99-016, the Emergency Network Security Policy for UC Davis. The emergency policy was issued as a temporary measure, out of urgent and immediate need, while a more inclusive network policy is developed.

A number of serious network abuses have occurred recently within the campus network: external attacks have compromised department computers, and non-university sites have been attacked from within the campus network. Examples of incidents include the use of university resources to illegally sell copyrighted material, an attack launched from a UC Davis library computer that took down an external Web site, and unauthorized access to a departmental server. A number of attempts to break into the campus network and secured campus computers are detected each day. Any of these attacks could cause severe damage to shared and individual electronic resources, such as email or computer files.

To understand the potential severity of a breach in network security, it's important to realize that if your computer is on while connected to the network, your hard drive is vulnerable to attack from any other point in the network. (This makes it especially important to back up your files if your computer is connected to the network.) It may be helpful to think of network security as the hull of a ship. A boat is only as sound as the thin layer separating what's inside from what's outside. Data corruption, loss and theft are all possible outcomes of a successful network attack. As the population of campus computer users grows, the number of tempting targets increases. This increases the likelihood that such damaging incidents will occur. So, unless steps are taken to protect the campus network, the risk continues to escalate over time.

Until February, no official policy existed to control and respond to network security breaches or violations. So, the Network Policy and Oversight Committee (NPOC) drafted the Emergency Network Security Policy immediately delegating network protection authority to the Network Operations Center (NOC). The NPOC plans to release an Interim Network Security Policy by the end of the 1998-99 academic year, with a finalized Network Security Policy scheduled for release in January 2000.

Developing a network security policy is a challenge, as the policy must not only foster sharing of computing resources, but also assist in minimizing risks to those resources. The final policy will address difficult and sensitive issues, and will therefore require extensive consultation with the campus community. As an institution of higher learning, UC Davis has a responsibility to serve as an example of a "good network neighbor" to the Internet community at large. The NPOC is deliberating on these issues as it moves toward a finalized Network Security Policy.

The Emergency Network Security Policy assigns the Network Operations Center (NOC) the purview to monitor network traffic and halt suspected network abuse. In the event of a potentially serious network incident, the Emergency Network Security Policy also grants the NOC authority to temporarily isolate systems, disconnect devices, and/or revoke network privileges. In cases where the local network administrator cannot be reached, or is unable to comply with a request from the NOC for assistance in trouble-shooting, network access may be suspended without notification.

These powers are aligned with the officially adopted UC Electronic Mail Policy and "Business and Finance Bulletin IS-3: Electronic Information Security" issued by the University of California Office of the President (UCOP). While enforcing this policy, every effort will be made to identify legitimate causes of peculiar network behavior before corrective actions are taken. The NPOC will act as a mediator in the event a system is inadvertently affected while trouble-shooting a potential network abuse and a formal complaint is made. Due judicial process will be provided to persons whose network privileges have been revoked. The final policy will require coordination between the NPOC and Student Judicial Affairs, Human Resources, the UC Davis Police, and other campus units that oversee the conduct of students, faculty, staff, and non-university individuals.

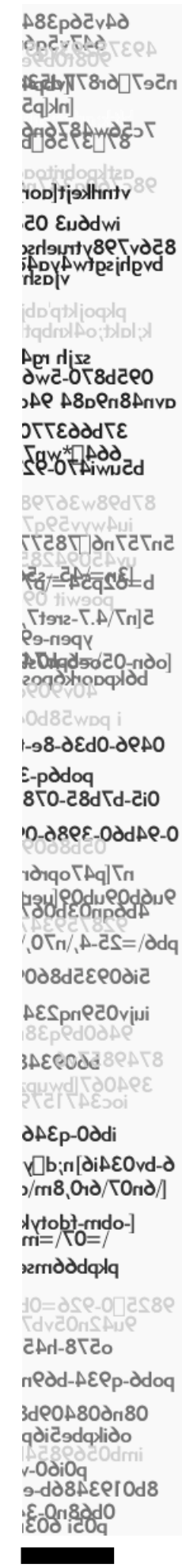
Wendy Phillips, Senior Writer with IT-Communications Resources, contributed to this article.

Plan of action to protect the campus network as outlined in the Emergency Network Security Policy

1. The Network Operations Center (NOC) monitors the network in order to detect potential network abuse.
2. The NOC and other campus units investigate when a network abuse is detected.
3. The NOC then promptly communicates suspected network abuse to affected network administrators and other groups as appropriate.
4. In the event a port is shut down, the NOC notifies the Associate Vice Chancellor of IT within 24 hours of the action taken and maintains records of network security activities.
5. The Network Policy and Oversight Committee mediates and resolves cases if issues arise from the above actions.

Resources

Please refer questions about the Emergency Network Security Policy to IT-Communications Resources Director Doug Hartline (*jdhartline@ucdavis.edu*) or Network Operations Center Manager Kevin Rhodes (*kcrhodes@ucdavis.edu*). For more information on electronic resources policies, including the UC Electronic Mail Policy (reissued March 23, 1998), the "Business and Finance Bulletin IS-3: Electronic Information Security" (issued by UCOP on November 12, 1998), and the UC Davis Acceptable Use Policy, point your Web browser to *http://it.ucdavis.edu/policies.html*.



Network attacks can result in data loss and corruption.

After Network 21, What's Next?

UCDNet2 Will Extend Campus Network

BY WENDY PHILLIPS

The Network 21 project officially concluded on December 18, 1998. Months before the end of Network 21, however, planning had begun on connecting those areas of the campus not reached by Network 21: UCDNet2 is the project launched from this planning.

Aiming for greater campus connectivity, UCDNet2 is designed to extend the network infrastructure to a number of campus locations outside the scope of Network 21, including outlying campus areas such as Research Park, located southeast of I-80, and facilities west of Highway 113. UCDNet2 will employ traditional copper wire, the fiber-optic infrastructure used in Network 21, and wireless technologies. In order to provide a low-cost solution to areas with existing telephone (copper) wiring, departments will have the option of using Digital Subscriber Line (DSL) technology to meet their connectivity objectives. These technologies will be re-evaluated over the course of the project to incorporate advances in networking technology. (For an explanation of DSL, see sidebar.)

The cost estimate for UCDNet2 was completed on November 8, 1998 and submitted to the Network Policy and Oversight Committee (formerly the Network21 Budget and Policy Oversight Committee). The committee is now in the process of determining the scope and funding of the project. Once this is determined, an environmental impact report and project plan will be prepared. Construction will begin after final approval. Because of the size of the project, the planning process will last through the end of 1999, with bids for construction going out in 2000. Actual trenching and installation of cable is proposed for late 2000. With its present design, UCDNet2 is planned for completion in 2001.

To keep you informed of the progress of this project, IT-Communications Resources is developing a UCDNet2 Web site. This site, which will describe the project goals and provide a map of proposed areas of expansion, will be available in early May.

Wendy Phillips is Senior Writer with IT-Communications Resources.

New Technology for Old Wiring: A Primer on Digital Subscriber Line Technology

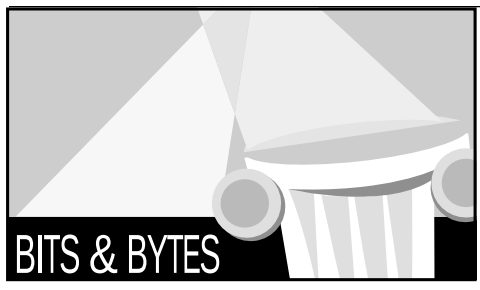
Digital Subscriber Line (DSL) technology can convert existing copper-wire phone lines into reliable network connections. DSL is being used in some cases where optimizing network speed is not vital and a lower-cost networking option (as compared to Network 21-style architecture) is desirable. The design of DSL for UCDNet2 will ensure that speeds of 1.5Mbps are available to those desktops served by it.

DSL's Advantages

- Creates a reliable, dedicated channel for 24-hour network access.
- Directly connects to the desired network without needing to initiate a dial-in sequence or telnet request.
- Doesn't require new cabling because it uses existing copper-wire phone lines to supply the network connection.

DSL's Limitations

- Data transfer rate is limited by the quality of the existing wire.
- As the distance traversed by the wire (from the walljack to the nearest central telephone facility) increases, the maximum data transfer rate decreases.



Software Site Licensing

BY LEIGH ANN GILES

New Software Web Site

http://software.ucdavis.edu

A new Web site with information about software licensing, system requirements, software descriptions, and downloads has been developed. The site combines information previously available on the IT Express, Site Licensing and Desktop Services Group Web sites. You can search for software by selecting an operating system or entering the name or type of program you need. This site is still in the testing phase, but if you get a chance try it out and let us know what you think.

Brio Users Group

The first Brio Users Group meeting was held in February. Van King, from Facilities Services, and Helen Paik, from Planning and Budget, described how they use Brio in their departments. (Brio is a data warehouse access and query tool.)

To subscribe to the Brio users email list, send email to *listproc@ucdavis.edu*, leave the subject blank and in the body of the message type: Subscribe brio@ucdavis.edu <first name><last name>.

For more information about Brio, see *http://slc.ucdavis.edu/slc/content/brio.html*.

Brio Virus Alert

A "Critical Alert" is posted on Brio's Web site indicating that the 5.5.5 update release CD contains a Power Mac specific virus. The virus can be detected and screened using the latest virus detection products. For more information and to read the Alert, go to *http://www.brio.com/support/bq5507.html*.

Juke Box Status

The CD Rom Juke Box, used to distribute specialized software to campus departments, is now equipped with a faster and more reliable hard disk. Departments must be registered with the Vendor Software Library (VSL) to acquire software at reduced prices from Oracle Corporation, Digital Equipment Corporation, Silicon Graphics, Inc., and Sun Microsystems. For more information about the CD Rom Jukebox and VSL, see *http://vsl.ucdavis.edu*.

Ghost

Ghost, a DOS-based program for "cloning" configurations, was recently acquired by Symantec, Inc., a major vendor of utility software for business and personal computing. The newest version of Ghost, 5.1c, is now available for download on the Web at *http://slc.ucdavis.edu/slc/content/ghost.html*. We will be renewing the license for updates for another year.

Anti-Virus Agreement

The UC Davis agreement for Dr. Solomon software has expired. Dr. Solomon is not fully supported by Network Associates, the company that recently acquired the anti-virus software. An agreement with Symantec should be in place by the end of March. In the meantime, if you need anti-virus software immediately, Wareforce Inc. is offering bulk pricing for most of Symantec's products. Wareforce's Symantec pricing is available at *http://www.wareforce.com/clients/uc_symantec.htm*.

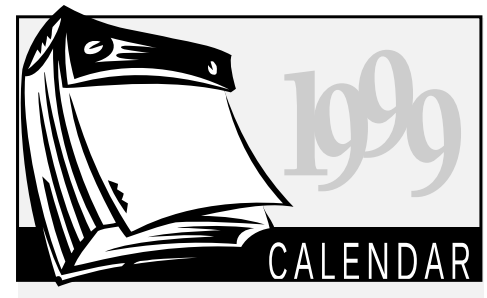
Other Symantec News

Symantec product pricing is listed on the Wareforce Web site at *http://www.wareforce.com/clients/uc_symantec.htm*. Products include Norton AntiVirus Desktop Solution, Norton AntiVirus Solution Suite, Norton Ghost, Norton 2000, and Norton Utilities. Wareforce will be pooling orders for Symantec products to reach the required minimum order quantities, and is requesting that each Symantec order contain only Symantec products. Wareforce will be tracking the quantities ordered and will report on its Web site when the campus has reached the minimum for each product. Wareforce will place the order only when the minimum is reached.

Statview

If you use Statview, a statistical program by SAS Institute, you will receive messages indicating that the software will expire in a few days. We are working on replacing this software with version 5.0.1. Purchase the license and CD for $45 at the UCD Bookstore Computer Shop. If you have more than one computer, you can purchase licenses individually without the CD for $40 per license. For more information, check *http://slc.ucdavis.edu/slc/content/statv.html*.

Leigh Ann Giles is the Campus Site License Coordinator. She can be reached at (530) 752-5413 or itslc@ucdavis.edu.



http://it.ucdavis.edu/itcalendar/

Visit the IT Calendar at the Web address above for the latest listings of technology-related events on campus (classes, presentations, workshops) and off campus (conferences and workshops).

Preparing for Banner's New Login Process

BY NICOLE COLLINS

On March 9 and 10, more than 300 campus members attended two presentations by several members of the Banner Upgrade project team. Jeanne Moje, from the Registrar's Office, discussed the campus's responsibility to protect the confidentiality of student records stored in the Banner Student Information System, as stipulated in the Family Educational Rights and Privacy Act (FERPA) of 1974. Dan Dorough, systems administrator with IT-DCAS, described the technical security issues and efforts underway to implement a single logon for all campus computing systems. Michael Buck, Banner project manager, ended the presentation with a live demo of the current and new login processes.

The New Login Process

If you are a Banner user, you should have received email notifications indicating that the new login process requires a Kerberos password and an Enigma Logic hard token. (For a complete checklist and instructions on how to prepare for the upgrade, refer to last month's issue of the *IT Times*, available on the Web at *http://it.ucdavis.edu/it.times/v7n4/banner.html*, or contact the Banner Help Desk at (530) 757-8996 or *bannerhelpdesk@ucdavis.edu*.)

Starting April 19, the only change you will notice when you access Banner is the new login process. Currently, you access Banner by entering your Citrix login (username) and Citrix password at the Banner screen. At the next screen, you click on the Banner icon, and then you enter your UCD LoginID and password. Finally, you click OK to run Banner at the Banner Logo Screen.

With the security upgrade, you will need to:

- Initiate the Banner login process by entering your Citrix login (username) and Citrix password at the Banner screen, as in the current login process.
- Next, instead of entering a database password, type your UCD LoginID and Kerberos password.
- A third window will request a password from your hard token. Take your token in hand, turn it on by pressing the ON button, wait until the window displays "EP" (for "Enter PIN"), and enter your assigned PIN (Personal Identification Number) on the keypad. A one-time password consisting of three characters, a dash, and three more characters will display on the hard token screen. You will have three chances to enter the correct PIN. After three failed attempts, "dancing lines" will appear on the token screen. They should disappear after one minute. If they do not, call the Banner Help Desk.
- Enter the hard token password at the Hardware Authentication Screen on your computer. (You may enter the characters as either upper- or lower-case, but you must omit the dash.)
- After you have successfully entered your password, Banner will start automatically. (See the tables below for a representation of the current and new login processes.)

Hard tokens, which look like small calculators, will generate a unique password every time you log on. This will prevent unauthorized access to Banner and will further protect the confidentiality of student records. They do not require any new software. In fact, they will enable you to log on to Banner from any workstation. Each token is assigned a serial number tied to an individual account, so it is important that you, and only you, use your hard token. You are responsible for any actions that take place in the Banner system under your account, so do not share your hard token with anyone and do not initiate multiple Banner sessions from several computers at the same time. Leaving one station unattended would create security risks.

Photo: Jim von Rummelhoff

Following a recent Banner upgrade presentation, Helen Rogers, right, from the Geology department, tries out a hard token under the watchful eye of veteran Banner user Claudia Turner, from the Veterinary Genetics Lab.

CURRENT LOGIN PROCESS	
Step	Action
1	Banner Screen Enter Citrix Login (username) Enter Citrix Password
2	Developer 2000 (Banner database) Screen Enter LoginID Enter Password
3	Banner Logo Screen Click OK to run Banner

NEW LOGIN PROCESS (Starting 4/19/99)	
Step	Action
1	Banner Screen Enter Citrix Login (username) Enter Citrix Password
2	Trust Broker Ticket Screen Enter UCD LoginID Enter Password (Kerberos)
3	Hardware Authentication Screen Enter Hard Token PIN Enter Hard Token Password Banner Starts

Visual representation of the current and upcoming Banner login processes.

Sign Up for a Workshop on the Web

If you have never used a hard token to access Banner or would like a quick refresher class, consider enrolling in one of the 45-minute workshops tentatively scheduled April 14-16 and April 19-21 in TB 134 (Macintosh Lab) and TB 135 (PC Lab).

The workshops are designed to help you

- Check your UCD LoginID, Kerberos password, and Citrix password.
- Obtain a PIN if you do not already have one.
- Practice using your security hard token.
- Try out the new login process.

Staff members will walk you through the login process and assist you with any remaining questions. If you decide to attend a workshop, bring your security hard token and a photo ID.

To sign up, go to the Banner training Web site at *http://registrar.ucdavis.edu/training* after March 30. The site will provide a schedule, including the times, days and number of seats available.

Due to SCT (the Banner software company) copyright concerns, access to the Banner training Web site has been restricted to the UC Davis domain. If you experience difficulty accessing the Banner training Web site from off campus (e.g., from the UC Davis Medical Center, Tulare, Bodega Bay, or Lawrence Livermore Lab), notify Jeanne Moje, from the Registrar's Office, by emailing her at *jmmoje@ucdavis.edu*. (Your computer's IP address must be registered with the Registrar's Office.)

Nicole Collins is Communications Analyst with IT-Information Resources.

NEED HELP WITH THE BANNER UPGRADE?			
Banner Help Desk	Ann Leamon	757-8996	*bannerhelpdesk@ucdavis.edu* *http://desktop.ucdavis.edu/projects/banner.html*
Programming hard tokens	Lisa Rocca	754-6207	*larocca@ucdavis.edu*
Banner accounts	Jeannie Marston	752-2984	*jsmarston@ucdavis.edu*
Banner upgrade workshops	Jeanne Moje	752-6732	*jmmoje@ucdavis.edu*
Banner Web site			*http://registrar.ucdavis.edu/training*

Configuring Eudora 4.0 To Access The Campus Modem Pools

If you accessed the Telnet-only Modem Pool to receive and send email before the pool was retired in early February, you will need to switch to one of the three campus modem pools (the Student/Staff Modem Pool, the Faculty Modem Pool, or the Legacy Modem Pool). If your computer is not already set up to connect to one of these pools, refer to the instructions available on the Web at *http://itexpress.ucdavis.edu/modems.html*. To access the campus network, you will also need to change your Eudora settings in order to send and check email. To do so, follow the instructions below.

Requirements

Before you configure Eudora to access one of the campus modem pools, you will need to verify that you have:

- A New-style UCD LoginID.
- A Kerberos password.
- The appropriate ServiceID for the modem pool you wish to access. (You need to obtain the IRAS ServiceID to access the 56K Student/Staff Modem Pool, and the IRMP ServiceID for the Faculty Modem Pool. The IMOD ServiceID associated with the 14.4K Legacy Modem Pool is automatically assigned to all UC Davis affiliates.)

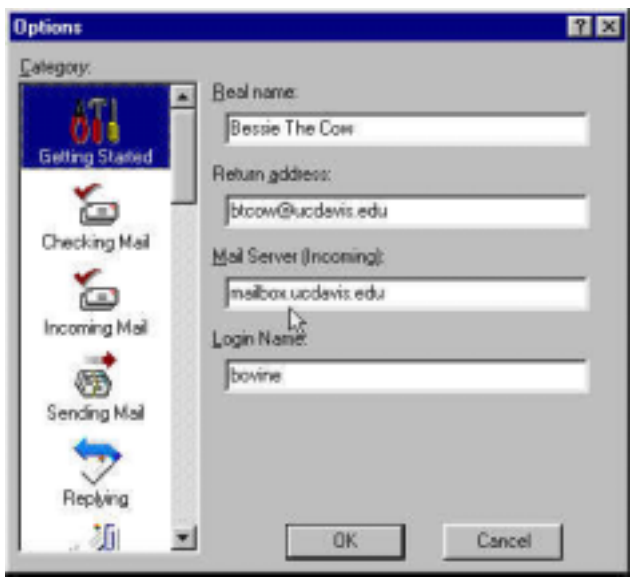
To acquire a new-style UCD LoginID, Kerberos password, and ServiceIDs, from your Web browser, go to the "Telnet Connections to mothra.ucdavis.edu" Web page at *http://mothra.ucdavis.edu/UCDLoginID/telnet.html* and click on the **telnet://mothra.ucdavis.edu** link. When you are connected to Mothra, type "services" at the login prompt, press Return (or Enter) to bring up the Mothra Services Menu, and select service option "G" to add one of the modem pools' ServiceIDs to your account. If your campus computer account does not have a new-style UCD LoginID or a Kerberos password, the system will prompt you to choose one. If you experience difficulty or prefer to talk to a technology consultant, please drop by IT Express in 182 Shields Library or call (530) 754-HELP.

- Internet communications software installed on your computer. Look for Dial-Up Networking for Windows 95 and 98, or for the Mac, either MacTCP and FreePPP or Open Transport TCP/IP and Open Transport PPP. (These can be downloaded from the Web at *http://itexpress.ucdavis.edu/modems.html*.)
- Version 4.0 (or a later version) of Eudora Pro. If it isn't already installed on your computer, you may download it free of charge from the UC Davis Software Web site (http://software.ucdavis.edu) or you may purchase Bovine Online, an Internet kit which includes Eudora Pro 4.0, other Internet applications, and a manual, all of which are customized for computing at UC Davis. The package sells for about $20 at the UC Davis Bookstore Computer Shop.

Instructions for Configuring Eudora Pro 4.0

If you meet all the requirements listed above, you will be able to configure Eudora using the instructions below. You will be prompted to enter or verify information about:

- Your UC Davis computing account.
- The email server (known as Mail Host or Delivery Host) to which your account has been assigned.



The Getting Started screen in Eudora Pro 4.0 as displayed on a PC (see step 5).

- The Simple Mail Transfer Protocol (SMTP) Server associated with your account (Step 11 below will help you determine what your SMTP server is).

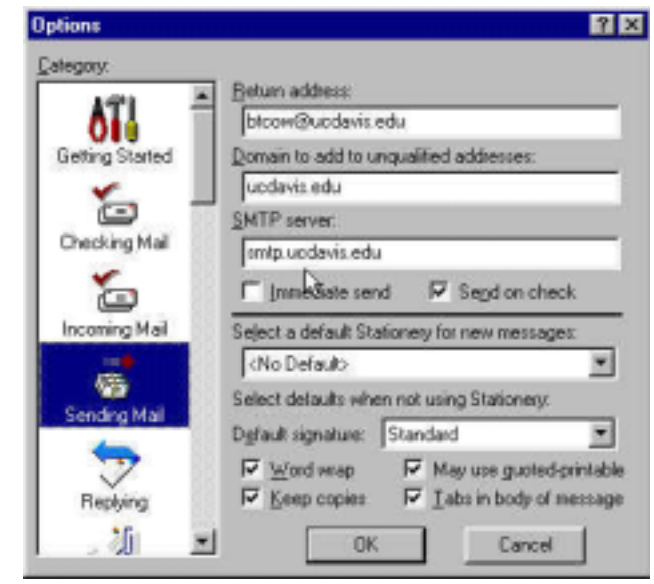
To configure Eudora Pro 4.0, follow these steps:

1. Look up your personal campus computing account information by using the campus Whois Service. Go to *http://www.ucdavis.edu/cgi-bin/whois/* and type in your last and first names, then press Return. You will see a screen similar to the one below, but with your personal information. (The screen will also include your title, department, and telephone number.)

   Example:

   ```
   Name: Bessie The Cow
   Email Address: btcow@ucdavis.edu
   Delivery Host: mailbox.ucdavis.edu
   UCD LoginID: bovine
   ```

2. After printing or writing down this information, start Eudora Pro.
3. Select Tools from the main menu (Macintosh users, click on Special).
4. Select Options from the drop-down menu (Macintosh users, select Settings).
5. Then click on the "Getting Started" icon on the left hand side of the window (see graphic at lower left).
6. From here, verify that your Username and Mail Server on the screen match the information presented in your Whois screen (see steps 1 and 2).
7. Your Mail Server from the Getting Started Settings screen must match the Delivery Host.
8. If you find a discrepancy, adjust the settings within Eudora Pro to match the information shown in the UCD Whois screen.
9. At this point, your settings for receiving email are configured.
10. To check your settings for sending email, click on the Sending Mail icon in the left scroll-down menu underneath the Getting Started icon (see graphic above).
11. Using the table below, verify that your SMTP Server box (the third box from the top of the screen) is filled in appropriately.



The Sending Mail screen in Eudora Pro 4.0 as displayed on a PC (see step 10).

Delivery Host (from Whois Service)	Corresponding SMTP Server (in Eudora Settings)
blue.ucdavis.edu	*blue.ucdavis.edu*
green.ucdavis.edu	*green.ucdavis.edu*
mailbox.ucdavis.edu	*smtp.ucdavis.edu*
scarlet.ucdavis.edu	*scarlet.ucdavis.edu*
yellow.ucdavis.edu	*yellow.ucdavis.edu*

12. Once you have verified the SMTP Server settings for sending email, click the OK button.

You should be all set to receive and send email through the campus modem pools. If you experience difficulty with any of these steps, contact IT Express at (530) 754-HELP or drop by 182 Shields Library.

IT TIMES

The IT Times is published by the Division of Information Technology, University of California, Davis, to inform the campus community and others of information technology services, facilities, and activities at UC Davis. It is distributed free of charge to members of the user community and to other universities. Use of trade or corporation names in this publication does not constitute endorsement by the University of California, Davis. IT Times articles may be reprinted as long as the source is accurately quoted and credited.

Editor: Babette Schmitt (530) 752-5965
Webmaster / Desktop Publisher: Richard Darsie
Senior Writer: Matt Peters
Designer: Marianne Post
Digital Imaging: Gabriel Unda

Information Technology UCDavis

Email: *itpubs@ucdavis.edu* Web: *http://it.ucdavis.edu/it.times/*