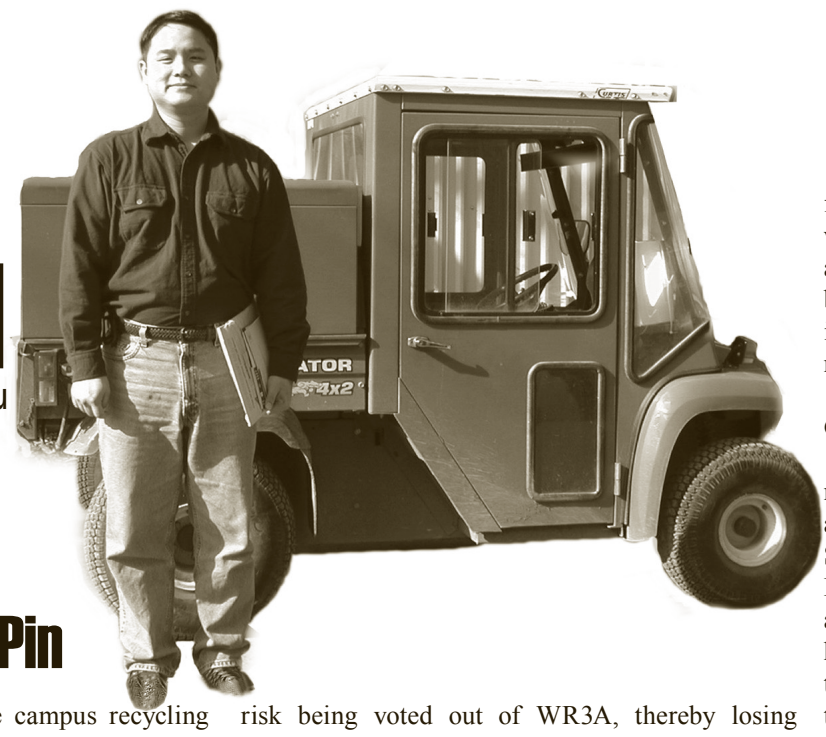
IT TIMES
http://technews.ucdavis.edu
Information and Educational Technology News for UC Davis
Winter 2005



UC Davis' Recycling King-Pin

The R4 trailer housing the campus recycling unit itself looks recycled. Located on a back road hidden from university traffic, its ragged front steps and old wood siding seem incapable of holding off the onslaught of winter storms. Inside, however, it's a testimony to the value of reuse: a cozy den, teeming with furniture and working students. Presiding over this environmentally-concerned crew is Lin King, Program Manager for R4 (Reduce, Reuse, Recycle, Rebuy), UC Davis' recycling headquarters. Although a soft-spoken man, King is passionate about the environment, both in his capacity as Program Manager and beyond.

He's also energetic. When asked how he came to the field of recycling, he tells a tale of circumnavigating the grounds of Cal State Fullerton while a graduate student there: "One day when I was finished with a Coke, I started looking around campus for a place to recycle the can. I literally walked the whole campus with a can in my hand until I realized there were no recycling bins *at all*. This is how I got started in my profession."

In his present position, King attends world-wide recycling conferences. At one such conference, he met Vermont-based waste recycler Robin Ingenthron, with whom he's now working on a nonprofit trade association designed to bring ethical standards to the e-waste recycling industry. The resulting World Reuse, Repair, and Recycling Association (WR3A) hopes to promote fair trade of recycled materials overseas, without sending "toxics along for the ride." The phrase refers to junk electronics not suitable for reuse or recycling that are included with recyclable material sent to countries with lax environmental laws. WR3A takes a strong stand against such practices, stressing that they undermine "charitable work, the environment, and sustainable employment." What this means is that any organization, whether buying or selling used electronics, must adhere to standards agreed upon by the association or risk being voted out of WR3A, thereby losing the organization's valued stamp of approval.

As a Chinese-American, King feels a particularly strong connection to the regions blighted by dishonorable recyclers (see *Asia Times* article: "Toxic US tech waste trashing Asia" available at www.atimes.com/media/DB28Ce01.html). What's more, his knowledge of Mandarin has already proven useful in overcoming language barriers with some Chinese recyclers. He now hopes to recruit foreign-born and visiting international students to contribute their translation skills in dealing with recyclers from other parts of the world.

Nine years ago, King returned to UC Davis, where he did his undergraduate degree, and now holds the position he once reported to as an R4 student volunteer. In between his undergraduate studies (Environmental Resource Science) and his present career, King worked as CSU Fullerton's first Recycling Coordinator. Upon receiving his MS at Fullerton, he worked for Orange County as a Staff Assistant in their Solid Waste and Recycling Department: "I handled environmental compliance issues at the landfill," he explains, a job that prepared him well for managing large-scale waste matters and for working with folks interested not simply in recycling but in cost-cutting as well.

King's master's thesis investigated the waste reduction and recycling programs at all 23 CSU campuses. "I realized," he explains, "that this was a needed document because there were limited resources available for campuses when I started the program." Fortuitously, the position at UC Davis became available just as King completed his degree in 1995.

King's campaign to educate the campus community about recycling continues apace. To learn how you might follow in King's e-waste recycling footsteps—without having to walk a mile to do so—read the article below. ◙

Science & Technology Merge in Sciences Laboratory Building

The Sciences Laboratory Building (SLB) has been in production for thirteen years, and the completed project turns out to be well worth the wait. The new structure features cutting-edge technology and the largest lecture hall on campus, as well as the UC system's first building completely dedicated to undergraduate laboratory instruction in biology and chemistry. But the Sciences Laboratory Building offers more than just new labs.

Catering to the Sciences

The Sciences Laboratory Building was created "to update and modernize laboratory teaching facilities for biology and chemistry," according to Tom Rost, Professor of Plant Biology and Chair of the Sciences Laboratory Building Committee. Situated on Hutchison Drive, the building is home to the UC Davis Center for Plant Diversity and Herbarium and the laboratory teaching programs for more than half a dozen science departments. Each of the new structure's 34 teaching labs is configured to operate media technology—features not typically present in other campus science labs.

The Sciences Laboratory Building also has a fully automated, computer-controlled greenhouse. Located on the third floor, the greenhouse is used for instruction by the Section of Plant Biology in the Division of Biological Sciences. A central computer controls the temperature, watering, and shading systems, and alerts greenhouse staff in the event that problems arise. Once the system is fully operational, staff members will be able to monitor and change greenhouse settings remotely from any location. Passersby can get a glimpse of greenhouse greenery from the third-floor hallway.

Biology 1A students prepare their labs in the new Sciences Laboratory Building.

Some of the most remarkable technology in the Sciences Laboratory Building, however, remains hidden from view. Lighting, for example, is automatically controlled to save energy while providing efficient light to lab benches. Features include motion detectors and the ability to turn lights off where daylight is available. In power outages, emergency power automatically provides minimal lighting and keeps critical building and laboratory services functional.

The building's automated fire detection system has 250+ alarms

See New Sciences Lab Building, back page

Worn-Out, Washed-Up, Unwanted

What You Should Do with Unwanted Computers: UC Davis' and Your Own

1. Learn about Wiping.

To rid your hard drive of data, you must overwrite the information rather than simply erasing it. Erasing a data file is akin to tearing out the chapter heading in a book's table of contents; the file directory no longer points to the data, but the data itself remains undisturbed. Likewise with reformatting, a process that eliminates most of the links between a hard drive directory index and the corresponding data areas. Overwriting, also called "wiping" or "shredding," is a process that replaces your information with random data, such as gibberish or zeros.

2. Obtain Wiping Software.

There are several utilities available for wiping data clean, including

- Autoclave: free from the University of Washington (staff.washington.edu/jdlarios/autoclave)
- Active@ Kill Disk: by LSoft Technologies, offered in both free and paid versions (www.killdisk.com)
- SuperScrubber by Jiiva: wiping software for Macs, available in two versions, beginning at ~ $ 50 (www.jiiva.com)

3. Rid your Computer of Personal and Official Information.

Using one of the above software programs, you should follow this process:

- Overwrite all data files.
- Overwrite your computer's operating system. This is typically performed by booting the computer from a diskette or CD containing overwriting software and then running the program against the hard drive.
- Overwriting is a multi-step process; make sure you overwrite your data at least three times.

4. Donate or Sell Your Computer.

If it's UC Davis equipment, send it to the Bargain Barn (752-2145). The folks there will assess your goods and figure out whether they can be refurbished and resold. If not, they will then be parted out or, in the case of worthless equipment, recycled as scrap.

If it's your own equipment, sell it on eBay or donate it via the National Cristina Foundation (www.cristina.org). If your home computer does not meet NCF's standards, check the California Electronic Product Collection Facilities site (www.ciwmb.ca.gov/electronics/Collection/) to learn about local recycling options.

Other Used Electronics

Unwanted cellphones, CDs, inkjet cartridges, and batteries can also be recycled. An R4 multibin designed to accept each of the above items is located in the MU, just inside the sliding doors and across from the newspaper racks.

Web Browsers

Dealing with Safety Issues and Finding a Browser that Suits Your Needs

Security vulnerabilities in Internet Explorer regularly make headlines all over the country; most notably, Penn State recently began to encourage users on their network to stop using IE altogether. Microsoft's practice of releasing free security patches draws some praise for the company's sense of responsibility, but leaves experts and average users alike questioning the browser's safety. Are these the concerns of over-anxious prophets of technological doom? Not necessarily. While it is possible to configure Explorer to be reasonably secure, IT Security Coordinator Bob Ono notes that, "doing so requires some careful consideration and most end-users avoid it as the process can be confusing." The most practical solution is to make a different browser your primary one and keep Explorer on hand in case you need it to access certain pages that can only be viewed in IE.

Fortunately, IT Express, the campus computing help desk, now provides technical support for several additional browsers, including Apple's Safari, the Mozilla suite (which includes a browser), and Mozilla's standalone browser Firefox. According to IT Express, campus computing services should function with each of these browsers.

It should be noted that installing a new browser does not require removing IE, and there are reasons not to do so. Windows users, in fact, cannot actually delete Internet Explorer because it is an essential part of the operating system, and Windows Update uses a special feature of IE called ActiveX that other browsers do not support. Even Mac users may want to keep Explorer (though Microsoft has stopped supporting the Mac version) as some Web sites do not work with other browsers.

Browsing Browsers

Before installing another browser or switching browsers altogether, you should first conduct research on the various models, says Ono, because the choices can be overwhelming; typing "Web browser" into Google, for instance, brings up 15 different programs in the first three pages of results.

One major criterion you should consider is whether the browser is maintained by a company—such as Netscape and Apple—that repairs bugs and provides regular updates. Because all browsers need updates, you should regularly check to make sure that you have the latest version. Finally, users can enable certain options that make a browser more or less secure, so you should learn about your new browser's safety features.

All of the browsers mentioned in this article, by the way, are available free. Most new Macintoshes come with Safari installed, and users of older Macs can download it at www.apple.com/safari. Mozilla and Firefox can be obtained from www.mozilla.org, and Mozilla itself is available on the MyUCDavis Software page.

Browser Features

In addition to increased security, other browsers may have useful features that Explorer lacks. One of the most popular is "tabbed" browsing – loading multiple Web pages in a single browser window to make organizing multiple windows easier. Many also block pop-up windows and offer a search bar (a feature available in Explorer with the Google Toolbar plug-in).

All-Around Security

Whichever you choose, a browser itself will not make your computing secure, though it can help. Installing and maintaining the right browser is an important step toward keeping your computer safe, but computing safely is a complex process that ultimately depends upon you, as a user, making the right decisions. You can find further help in your effort to keep your computer safe by consulting "Ten Steps to Safe Computing" found at http://security.ucdavis.edu/security101.cfm. ◙

What to Look A

Tabbed Browsing

This feature allows multiple Web pages to be opened in a single browser window.

Web Downloading Control

Some browsers feature controls that inquire where you would like downloaded programs to be placed; this option could prevent files from being downloaded onto your computer without your knowledge.

Pop-Up Window Blocker

This feature automatically stops small pop-up windows from appearing, and permits you to override it for certain sites.

	Operating System	Compatible with DaFIS, DistAuth, MyUCDavis & SISWEB	Pop-Up Window Blocker
Internet Explorer	Windows	✓	Included in Windows XP SP2
	Mac (discontinued)	✓	✗
Mozilla Firefox	Windows	✓	✓
	Mac OS X	✓	✓
	Linux	✓	✓
Mozilla	Windows	✓	✓
	Mac OS X	✓	✓
	Mac OS 9 (up to 1.2.1)	✓	✓
	Linux	✓	✓
Apple Safari	Mac OS X	*	✓

* Off campus users may experience difficulties using Safari with MyUCDa

** Available as a third-party plug-in

SPYWARE . . . Your Computer May be Watching You

Surfing the Internet one night, you Google song lyrics to use in a birthday card you're making, and then click on the link to a promising site. At the front page, pop-up windows bombard your screen faster than you can close them. In the midst of them is a security message from Microsoft asking if you want to install a new patch. Figuring this might be the solution to all those pop-up windows, you click "OK." Later, however, you discover mysterious icons on your desktop, and they return even after deleted. What's more, your homepage has been reset to a search engine you've never heard of, and your computer is running a lot more slowly than it used to. Sound familiar?

Unfortunately, to many people it does. That "patch" wasn't a software update, but a vicious program known as spyware. Threatening your privacy as well as your computer, spyware hogs system resources and causes other software to crash.

What is Spyware?

Spyware is software that gathers information about your habits and reports the data to unscrupulous companies or individuals. Data recorded can be as general as the Web sites you visit or as specific as the keystrokes you enter.

What is Adware?

Spyware encompasses other types of malicious software, such as adware, which displays ads–often as pop-up windows in Web browsers. Though legitimate programs, such as AOL Instant Messenger, feature adware, they are forthright about their content, displaying ads in the program window itself and selling ad space in lieu of charging you a fee for the program. The majority of adware programs and all spyware programs are not so upfront, and therein lies the problem in detecting them.

What Does it Look Like?

Adware and spyware programs distribute their undesirable content in many ways. The most popular form of spyware is innocuous-looking free software that offers to perform such functions as searching the Web or displaying weather information. A multi-page End-User License Agreement buries in confusing legalese references to programs that monitor the user's activities. Spyware may also be hidden in pirated software downloaded free or sold over the Internet. Other spyware programs present themselves as browser plug-ins or important software updates; these often appear among other pop-up windows that try to confuse the user. Sometimes, they may even download themselves surreptitiously; if a user's security preferences are set low enough to allow programs to download automatically, spyware can enter the computer undetected.

What's a Person to Do?

The best solution to the problem of spyware is to avoid downloading it; don't use pirated software and be sure to read End-User License Agreements for free programs before accepting them. While this can be time-consuming, it will save you the significant

or in a Browser

Third Party Cookie Blocking

is feature blocks cookies from sites you n't actually visit, but that are connected in me way to sites you do – for example, from vertisements on sites you go to.

Site-Level Cookie Control

Most browsers can block cookies, which are small pieces of data that Web sites use to keep track of your surfing habits at those sites.

SSL Certificate Checking

Some browsers are able to check the validity of an SSL certificate (an electronic signature that identifies a site as trustworthy) and warn you of untrustworthy or revoked certificates.

Site-Level Cookie Control	Third-Party Cookie Blocking	Tabbed Browsing	Web Down-loading Control	SSL Certificate Checking
✗	✓	**	✓	✓
✗	✗	✗	✗	✓
✓	✓	✓	✗	✓
✓	✓	✓	✗	✓
✓	✓	✓	✗	✓
✓	✓	✓	✗	✓
✓	✓	✓	✗	✓
✓	✓	✓	✗	✓
✓	✓	✓	✗	✓
✗	✓	✓	✗	✓

vis Course Management features (e.g., GradeBook, final grade submission, uploading files).

amount of time you would have spent uninstalling spyware.

If you use Internet Explorer, increase your security level to at least "medium" and ask it to prompt you every time you run ActiveX controls. If you need help with this, contact IT Express at 754-4357 or ithelp@ucdavis.edu, or consider switching to another browser (see "Web Browsers: Dealing with Safety Issues and Finding a Browser that Suits Your Needs," page 2).

Last, but not least, download anti-spyware and anti-adware programs. As with antivirus programs, these should be run and updated regularly. If spyware is already present on your computer, a single program will not, as a rule, catch all of it. You will probably need to use several anti-spyware programs, but because many are free, this shouldn't prove costly.

While spyware is a dangerous threat, it needn't prevent you from surfing the Web. With a bit of attention, you should be able to avoid downloading it, and anti-spyware and anti-adware will remove what you don't catch. Spyware is a problem that's not likely to disappear anytime soon, but with diligence, it is a manageable risk of Internet use.

For more information on this topic, see the UC Davis Security Web site pages on spyware and adware at security.ucdavis.edu/101_spyware.cfm and security.ucdavis.edu/101_adware.cfm, respectively. ◙

(DON'T) Go Phish!

Do you know how to spot a "phish" out of water? It looks like an email from Washington Mutual, informing you that your bank account will be closed if you don't respond *immediately*. Phishing scams such as this target Internet users of all ages and skill levels, and ruthless con artists dedicate themselves to acquiring personal information such as credit card, bank account, PIN, and social security numbers. But if you learn how to identify phishing scams, you should be able to avoid the stress involved in undoing identity theft.

What Is Phishing?

The term "phishing," first coined by hackers in 1996, refers to the process by which hustlers use email or other "lures," such as instant messages and chat-rooms, to fish for personal information from unsuspecting computer users. Recent businesses targeted by phishers include America Online, eBay, Paypal, Earthlink, U.S. Bank, and the aforementioned Washington Mutual.

Identifying a Phishing Scam

Phishing messages often share characteristics, so you can protect yourself by learning to recognize some of the features of a typical phishing email:

- *Authentic-Looking Graphics*: Appropriate graphics are easily duplicated and their presence does not mean the email originates from a trusted business.
- *Threatening Tone*: Alarming statements—claiming, for instance, that your account will be closed or you will be fined unless you act *right now*—should ring an alarm of a different sort; a legitimate business is unlikely to conduct such business over email. Call the established business telephone number to confirm the email's authenticity.
- *Personal Information Request*: Most legitimate businesses will not ask you for information such as passwords, account numbers, or PIN numbers via email or Web form. Again, rather than responding to the email, call the established business telephone number to confirm that the message is official.
- *Misleading Links*: Using a process called "masking," phishers create a legitimate-looking link (e.g., Paypal.com) that actually takes you to a different address (e.g., auth.BestDealsMarketBanking.tk/paypal). To avoid "masked" links, open your Web browser and type the legitimate link yourself.
- *Grammar and Spelling Errors*: Spelling mistakes can be part of a strategy used by phishers to avoid spam filters or can indicate that the lure originates outside the country and the phishers don't fully understand the grammar standards used by the business they're mimicking.

False Web Sites

Most phishers will direct you to a Web site designed to collect your personal information—a site not authorized by the mimicked business. There are a number of warning signs that will help you spot a phisher's site before accidentally disclosing private data:

- *Make sure the site is secure*: A Web page graphic that simply tells you it's "secure" is not enough, especially when you're submitting personal information. Secure sites most often contain a small image of a lock in the bottom right corner of the browser window frame.
- *Pay close attention to the URL of the site you are visiting*: Here is an example of a phishing URL: http://visa.com/?rDirl=http://200.251.251.10/. The initial part of the address makes it appear that the link connects to Visa, a legitimate credit card company. If you look at the last half of the link, however, you'll see that the second "http" will redirect you to a different site. Also, look for an "s" for "secure" following the introductory "http"; that is, it will read "https."
- *Avoid Web sites that don't have domain names*: When you see a Web site address containing an IP address—four sets of numbers separated by periods (e.g., 200.251.251.10)—you should be wary. Most scammers mask their identity by giving these numbers instead of an actual domain name, such as "www.google.com."
- *Watch out for browser errors and rendering errors*: If your browser notifies you that a site contains "rendering errors," you should be skeptical. It is very rare that a legitimate site will have such errors.
- *Keep your computer up to date*: As vendors uncover new scams, they release updated "patches" designed to fix vulnerabilities in your system. Use these. Many new operating systems will check for and download updates automatically.

If You Think You've Been Taken…

Take action as quickly as possible. Whatever information you've shared, you'll find the proper actions to take at www.antiphishing.org/consumer_recs2.htm. Even if you haven't divulged personal data, you can help in the fight against phishing by reporting fraudulent sites on the FBI's Internet Fraud Complaint Center at www.ifccfbi.gov/index.asp. Click on the "File a Complaint" link. For specific examples of phishing fraud and the tactics used, visit the UC Davis Computer and Network Security site (security.ucdavis.edu/101_phishing.cfm) or the industry-based Anti-Phishing Working Group (www.antiphishing.org/phishing_archive.html). ◙

New Sciences Lab Building

continued from front

and visual strobes to alert occupants while at the same time sending a message directly to the UC Davis Fire Department. What's more, the building's mechanical systems automatically go into prevention mode to help stop the spread of smoke.

Something For Everyone

Not every part of the SLB is geared toward those interested in the sciences. The building's wireless lounges and discussion rooms, for example, are set up so that you can surf the Web with your laptop. And beginning Spring 2005, Bio Brew, SLB's in-house coffee shop, will vend snacks and caffeine for hungry and sleep-deprived visitors.

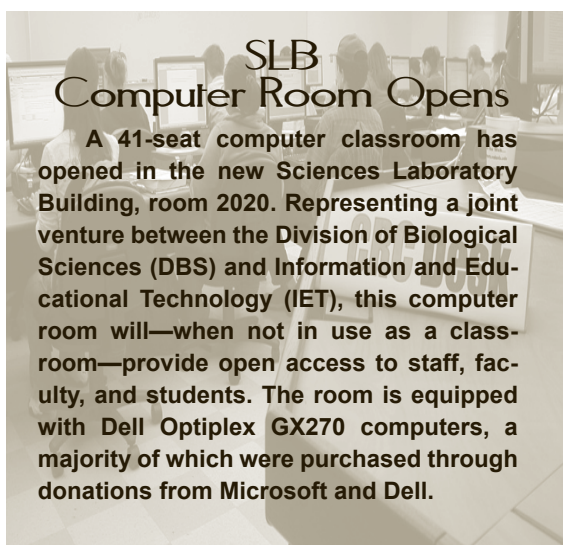
The opening of the SLB also marks an addition to the campus computer rooms. One computer classroom will be open to students, faculty, and staff when classes are not in session, and a second computer laboratory—to be completed next year—will specialize in bioinformatics.

The Biggest Lecture Hall on Campus

The Sciences Lecture Hall 123 features three large-video screens.

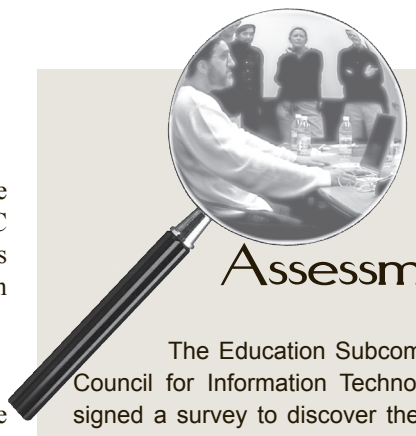
The new lecture hall is located adjacent to the SLB. Not merely the largest UC Davis lecture hall, the lab also features the finest in technology. The 517-seat hall boasts the highest-definition (DVI) data projector on campus, projecting images with greater clarity and detail than any other campus projector. And the hall is home to three video screens, so the system could be expanded in the future to allow simultaneous display of up to three different videos or images. "An instructor could eventually display an overhead transparency, a Web site, and a PowerPoint presentation from her laptop all at the same time," explains Rost. The lecture hall also features remarkable acoustics; students in the last row of the lecture hall can hear a professor clearly even if the professor is not using a microphone!

Although currently used only for classes, there is a possibility that in the future the hall could be reserved for non-class use. Rick Sprunger, who oversees the Classroom Technology Team, proudly proclaims that "this lecture hall showcases the campus' best technological abilities." ◙



SLB Computer Room Opens

A 41-seat computer classroom has opened in the new Sciences Laboratory Building, room 2020. Representing a joint venture between the Division of Biological Sciences (DBS) and Information and Educational Technology (IET), this computer room will—when not in use as a classroom—provide open access to staff, faculty, and students. The room is equipped with Dell Optiplex GX270 computers, a majority of which were purchased through donations from Microsoft and Dell.



LEAD II: Faculty Needs Assessment Survey

The Education Subcommittee of the Campus Council for Information Technology (CCFIT) has designed a survey to discover the needs, interests, and most useful IET resources of UC Davis faculty—both federation and academic senate. CCFIT Chair, Professor Caroline Bledsoe, points out that "faculty are spending more and more time using information technology in research and especially in teaching." She requests that faculty fill out the survey (available now at learning.ucdavis.edu/LEAD), "so CCFIT and IET know how best to help you."

2005 IT Security Symposium

UC DAVIS

Sponsored by UC Davis Information & Educational Technology and University of California: Office of the President

Planning for the 2005 IT Security Symposium, scheduled for June 22 – 24, continues. The planning committee is happy to confirm Scott Charney, Microsoft Chief Security Strategist, as the keynote speaker. The committee is putting the finishing touches on the event schedule, and registration is expected to open in early April.

The $100 per person fee will include attendance at the welcome reception, keynote speaker presentation, instructional lab and vendor sessions. Also included are conference publications, lunches and daily refreshments, and an event t-shirt.

For additional information and to register in April, visit itsecuritysymposium.ucdavis.edu/. If you have questions about the 2005 IT Security Symposium, please contact Robert Ono, IT Security Coordinator, at raono@ucdavis.edu.

SISWeb Materials Online

Lana Dancy, IET Banner SIS Trainer, recently conducted a SISWEB course for which she is now offering a class handout online. *SISWeb: The Student's Perspective*, was presented in November and December, 2004. Designed to help staff members who "find it difficult to assist students with their SISWeb questions," the course gives staff a student's view of the SISWEB system. The URL for the handout is www.bannertraining.ucdavis.edu.

Dancy will soon be offering additional Banner classes and can be contacted via email (lrdancy@ucdavis.edu) or telephone (757-3278) for further information. For additional Banner training needs, feel free to contact Dancy.

SIS DS: Web Interface Allows Easier Viewing of Student and Course Statistical Reports

Thanks to a partnership between the Office of Resource Management & Planning (ORMP) and IET, a new Web application has been developed that will improve access and viewing of campus reports. Called Student Information System Decision Support (SIS DS), this system, which has an interface similar to DaFIS DS and PPS DS, will support basic reports for a wide range of student and instruction-related data. The initial reports focus on course section information, student course enrollment and instructional workload statistics (available at https://sisds.ucdavis.edu or the SIS DS link under the "My Office" tab in MyUCDavis). Access has been granted to all staff and faculty.

Campus members are encouraged to contact the team to discuss how their reports can be included in this new system. Suggestions will be coordinated with management and the Campus Data Stewards. Send comments or report requests to sisdshelp@ucdavis.edu.

Online Grading Deemed a Success

As of Fall 2004, online grade submission became mandatory for course grades. How has the program worked for those new to it? Over 150 instructors weighed in when uploading their grades last quarter and comments were, by and large, very positive.

What's more, Interim Registrar, Lora Jo Bossio, reports that "the reduced workload in the Registrar's office due to the online grading system allowed us to provide grades to students and staff more quickly than in past years."

IET Mediaworks, which has provided support for online grading, continues to make improvements to the system. For Winter Quarter, this includes making it easier for instructors who teach large courses to grade multiple course sections simultaneously.

Web-Based Departmental Faculty Directory Now Live

Following up on a request from Provost Virginia Hinshaw, IET-Communications Resources and the IET-Middleware Team worked together to develop an online directory index of UC Davis faculty by department and rank. The directory can be found at www.ucdavis.edu/search/faculty.

Media Cabinets Help Instructors Spice up Their Lectures

Very few universities in the country offer media technology hookups in every single classroom, but as of June, 2004, UC Davis is proud to be among the few that do. The media cabinets present in all 116 general assignment classrooms are configured to the campus computer network and allow instructors to access the Web, outline presentations, play music and movies, and share files from their laptop computers.

The campus began installing the "plug and play" media models five years ago. The design was chosen for user-efficiency, ease of upgrades and technical support. The cabinets are improved as new technology enters the market and as the campus budget allows, ensuring that UC Davis instructors receive the best quality equipment. According to IET Classroom Technology Services (CTS) Director, Jan Dickens, "the data projectors are currently being upgraded in general assignment classrooms across campus."

CTS offers technical support assistance for instructors using the classroom equipment. A plaque with the "classroom hotline" phone number (752-3333) is displayed near each media cabinet, and the operators who answer will provide either phone support or in-person assistance, as appropriate. A do-it-yourself troubleshooting guide is also located near each media cabinet. The guide offers help on various topics, such as operation of the DVD player, and assistance with more complex subjects, such as color calibration.

CTS also holds training sessions for lecturers, professors, TA's and departmental technical support right before the start of each quarter. Instructors are invited to bring their own computers to the training sessions, which are scheduled in general assignment classrooms. According to Dickens, such training will help professors be ready to go the first day of class. "Our mission is to make the teaching/learning environment the best it can be at UC Davis, both for the teacher and the learner. We survey all teachers at the end of every quarter seeking feedback and recommended improvements." For information on the next training session or to submit suggestions, visit the CTS Web site at cts.ucdavis.edu. ◙

TechNews

http://technews.ucdavis.edu

The IT Times is a companion to TechNews, a Web site providing up-to-date information and educational technology news for the UC Davis campus community. Visit technews.ucdavis.edu to read the latest stories, and click on "Subscribe" to have the headlines delivered straight to your in-box.

The IT Times is published by the Office of the Vice Provost - Information and Educational Technology. All content and design is produced by IET staff, unless otherwise noted. The IT Times is distributed free of charge to 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 quoted and credited accurately.

Please send story ideas and comments to Nancy Olsen, Editor

ietpubs@ucdavis.edu