Information Technology News for the UC Davis Community

IT TIMES

Fall 2008

Open and shut

We're a public research university. We can't lock away our IT network the way a private company can. Neither can we let it admit viruses, or leak private data to identity thieves. Bob Ono discusses how the campus reconciles access with security, describes what's ahead in 2008-09, and explains why the health of the whole enterprise depends on you.

Did you receive any of the seven or eight phony "UC Davis" emails this year? The ones with tilted grammar that warned of trouble, sent from concealed sources that asked for your email account name and password? Phishing messages like those are one reason why the campus employs Bob Ono. Helping to deter online fraud is one of his responsibilities as coordinator of information technology security at UC Davis.

Ono knows the campus pretty well. He earned a bachelor's degree in health-care administration (an independent major) here in 1976, worked in the ASUCD Coffeehouse, was elected to the student Senate, lives in Davis, and is the husband of one alumna and the father of another. But he was hired eight years ago from the Sacramento Municipal Utility District, where he was information security officer, for what was then a new position at UC Davis, because of his skills in IT security.

He says, in his quiet and engaging style, that IT security is everyone's job. Its strength at UC Davis relies on collaboration, from consulting with faculty, staff and students on security programs, policies and priorities; to individuals choosing strong passwords; to Ono sharing information and resources with campus IT peers nationwide so that all of them can more easily anticipate the threats and challenges ahead.

UC Davis is a major research center, so IT security here requires more than a tight defense. It requires a secure but generally open computing network, accessible to faculty, researchers, students, employees and affiliates around the globe. In late summer, Bob Ono talked about the work with IET senior writer and editor Bill Buchanan.

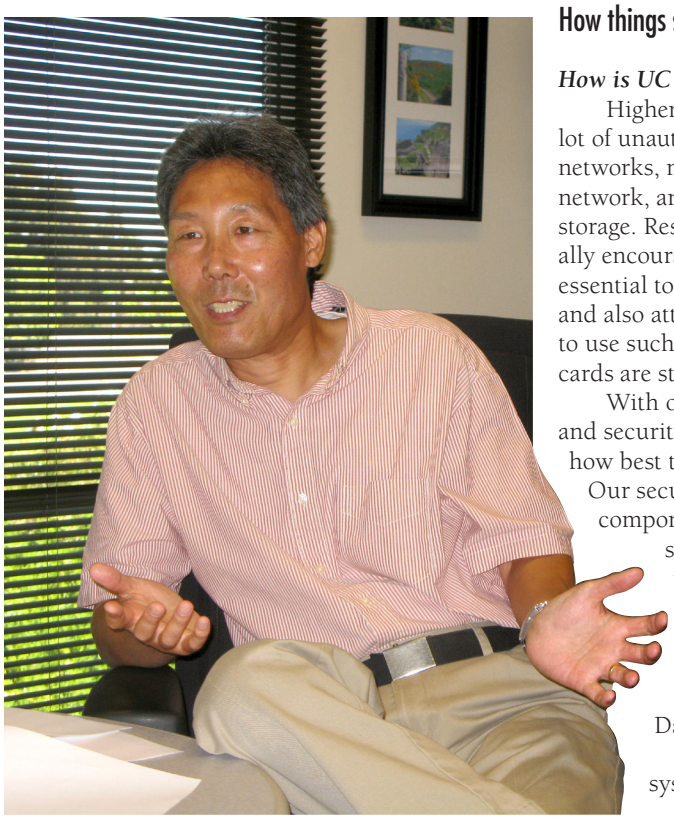

Photo of Bob Ono by Dennis Ngo

How things stand

How is UC Davis doing in IT security?

Higher education institutions attract a lot of unauthorized activity. We have fast networks, many computing hosts on the network, and tremendous amounts of disk storage. Research programs have traditionally encouraged open networks. They're all essential to higher education technology, and also attract individuals who would like to use such services for mischief. So the cards are stacked against us a little.

With our campus cyber-safety policy and security program, we have looked at how best to address the security threats. Our security program is based on four components: prevention, through policy, standards, and use of security technology; quality assurance; incident investigation and detection; and recovery.

I think, with our very comprehensive program, UC Davis is doing pretty well.

The security of our computing systems and network will

See Security, page 6

In this issue:

Photo: Leslie Mudsen-Brooks

Dawn Sumner at the Summer Institute on Teaching and Technology. **Part of summer recap, Pages 4-5**

IT TIMES CHANGES

We're moving online.

After this issue, the 16-year-old *IT Times* newsletter will be distributed electronically, instead of by campus mail, to save money and paper.

The content isn't changing. *IT Times* will keep focusing on news and information about campus tech at UC Davis, with the goal of explaining how that technology can help staff and faculty do their work. The newsletter will also continue as a periodical companion to *TechNews*, a campus information service for students, faculty and staff that posts items online every week.

The electronic *IT Times* will be produced as an 8.5x11-inch PDF that readers can print easily (we adopted the smaller size with this issue). To receive a notice when each issue is ready, please subscribe to free *TechNews* updates at technews.ucdavis.edu.

Questions? Email Bill Buchanan at wrbuchanan@ucdavis.edu. ■

Student email switches to Gmail-based DavisMail

UC Davis, meet DavisMail. It becomes the campus email service for students starting this fall.

On Oct. 6, the campus began moving more than 32,000 undergraduate and graduate email accounts from the old system, Geckomail, to DavisMail—a renamed version of Gmail, the free service from Google Inc. The Gmail advisory group chose the name because it links the service with the campus and should remain a good fit as UC Davis continues to grow and diversify.

The switch from the Geckomail gives students an email system with much more data storage and features, plus access to popular communication tools in Google Apps for Education. Faculty and staff email accounts are not moving to DavisMail, although the campus will discuss that possibility later.

Students will keep using their existing ucdavis.edu email addresses. They won't need to do anything to assist the transition except accept Google's terms of service agreement. Students can opt out of DavisMail but will have to choose an alternative service such as those provided by Microsoft or Yahoo. All of that is spelled out in email messages the students have received this quarter.

Information and Educational Technology (IET) hopes to move all the student accounts to DavisMail this autumn, but the task could extend into early 2009. The accounts will move in batches, starting with some graduate students.

Other key points:

• IT Express, the Campus Computing Services Help Desk, will support use of DavisMail. Google Apps will be supported by Google.

• Each account will have upwards of 7 gigabytes of data storage, more than 100 times greater than Geckomail offers.

• Students will access email through the MyUCDavis Web portal.

• The switch affects all undergraduate and graduate students, except for UC Davis Medical Center students, who use UC Davis Health System mail systems.

• The change will not affect students' contact information in WarnMe, the campus emergency alert system. That's because their UC Davis email addresses are not changing.

IET tried Gmail with about 300 students in winter 2008, then followed up with months of review and discussion with key groups across campus. Students praised the service in surveys.

In June, the University of California Office of the President signed a systemwide, seven-year, Gmail contract with Google, which is providing the service at no cost to the university. The agreement gives UC Davis exclusive control of UC Davis email accounts, and lets the campus back out of the relationship at any time. Davis is the first campus in the system to adopt Gmail.

An oversight committee will help steer the transition to DavisMail. It includes representatives from the Associated Students of UC Davis, Office of Student Affairs, Alumni Association, University Communications, the Deans' Technology Council, and IET. ■

Privacy is protected

As required by federal law and university policy, the university will not share personally identifiable confidential information with Google or any other third parties. An ad hoc privacy committee at UC Davis reviewed the Google agreement, and found no concerns that prevent using the service here.

READ MORE:

Learn more at davismail.ucdavis.edu.

Adobe Connect Pro helps UCD'ers skip travel

Two-way video and voice connections via the Internet, and the ability to share documents and applications online, are not new. But combining those features into one convenient package makes online collaboration easier and more attractive.

That's the idea behind Adobe Connect Pro, a program available on campus from Information and Educational Technology's Academic Technology Services unit. For a fee, the Adobe software offers users a virtual meeting room where people can sign on easily from their own computers, see and talk to each other, mark up documents together, share applications and desktops, and more.

"There are a lot of advantages to using Adobe Connect Pro, especially for people who need to meet often but are separated by many miles or even continents," said Earl Schellhous, lead programmer for the project.

"You can have video and voice-over-IP sound [voice over Internet Protocol] in Adobe Connect Pro, as well as live text chat," he said. "You can share PowerPoint presentations, white boards, images, files, and even applications on your computer."

The program resembles such existing programs as Microsoft Live Meeting, Elluminate, or Webex, and runs on Flash Player, which almost all computers have, Schellhous said.

To start a meeting, hosts create a meeting area with a secure Web address, invite participants, and tell them when to sign on. From there, participants use the array of tools as needed.

Adobe Connect Pro "is rapidly becoming a strategic part of our broadly distributed organization," said Bob Sams, director of Communication Services for Agriculture and Natural Resources. Sams likes, among other factors, the quality of connection and ease of use.

"With the increases in travel costs, and the increased value of ANR and UC Davis faculty and staff time, Connect is quickly becoming a very good way to make a presentation or participate in a distant meeting without leaving the office," said Mike Poe, media services manager for ANR Communication Services.

UC Davis clients have found several ways to employ the program. It has been used for rounds at the UC Davis Medical Center and for online classes, Schellhous said. "Language departments can use it to hear a students' pronunciation in a live session," he added.

Cancer pathologists Dr. Robert Cardiff and Dr. Jose Galvez use Connect Pro to work with other cancer research groups worldwide.

"Since pathology is an image-intensive discipline, we frequently share slides using whole slide images over Breeze [an earlier name for Connect Pro]," Cardiff said.

"The most off-campus participants come from monthly meetings with a breast cancer research group," he said, "with participants from Philadelphia, New York City, Montreal, Oxford, Davis, and Sacramento." ■

READ MORE:

To set up an Adobe Connect Pro account, contact Information and Educational Technology's Academic Technology Services at (530) 752-2133 or ats@ucdavis.edu. The service is available to UC Davis users on a recharge basis, at departmental or individual rates. Read more at iet.ucdavis.edu/teaching/commtool.cfm.

182 Shields converted into newest computer lab

Information and Educational Technology has converted the former home of the IT Express walk-in desk, 182 Shields Library, into a computer lab. The change accompanies an expanded availability of the password reset feature that was the most popular service offered at that location—and adds more open-access computers and printers to a campus that needs them.

The room closed as an IT Express location Aug. 15. Low walk-in traffic, the chance to better meet students' needs for computer access, and the ability to reset passwords at more locations sealed the deal.

The re-opened 182 Shields now has 38 computers (including an ADA/accessible computer station), plus printers, and has been added to the wireless printing network. (Learn more about that service at wirelessprinting.ucdavis.edu.)

The room proved instantly popular. In its first two weeks, it attracted 10,560 visits, enough to rank as the second-busiest of Computer Lab Management's 18 computer rooms. (MU Station came first with 15,856.)

Demand for computer stations keeps growing as instructors and students make greater use of technology in their work. Classroom Lab Management, the unit of IET that runs the computer labs, "recorded the highest number of total logins and reserved computer classroom hours in our history" in spring 2008, according to its spring 2008 quarterly report. This fall, log-ons to computers in all of the rooms combined are running about 1,050 per weekday higher than they were a year ago.

The library already hosts a computer lab in 163 Shields. IET appreciates the library's willingness to share its space and allow computer labs in both 163 and 182 Shields, said Liz Gibson, director of Academic Technology Services in IET.

Meanwhile, password resets for faculty, staff and students can now be done during more of the day at several computer labs across campus: 182 Shields (the service was temporarily available in 163 Shields this summer); MU Station; 1154 Meyer; 15 Olson; 1101 Hart; and 75 Hutchison.

The reset service will be available from 8 a.m. to 9 p.m. Monday-Thursday, and from 8 a.m. to 6 p.m. on Fridays. The service will not be available when the rooms are closed, so please check individual computer lab hours at clm.ucdavis.edu/rooms.

Contact IT Express, the Campus Computing Services Help Desk, at (530) 754-HELP (4357). ■

Photo: Phil Riley

Evan Morgan and Peter Wagner help prepare 182 Shields in late September, shortly before the former IT Express walk-in location re-opened as a new open-access computer lab. It attracted 876 users on Sept. 25, the first day of fall classes.

Create new campus computing accounts online

Some departments often send new employees to 182 Shields to create their campus computing accounts. That's not necessary, because the task can be easily handled online, from anywhere. Go to accounts.ucdavis.edu, select "Get your UC Davis Computing Account," and follow the step-by-step instructions.

SmartSite focuses on improving Gradebook

SmartSite kept growing over the summer, gaining ground on its long-term goal of becoming a widely used online resource that can help UC Davis faculty, staff and students teach, research, and collaborate.

The SmartSite group installed a software upgrade with minimal disruption, boosted its training outreach to campus departments, and hosted a well-attended session for administrators in early July.

They also kept plugging away at the top remaining priority for 2008-09: improving its Gradebook digital grading tool so that it will work at least as well—and in fact, will work far better—than the one available through the MyUCDavis course-management tools. Once the SmartSite Gradebook hits that performance mark for a year, the campus intends to retire all the MyUCDavis course tools. (The portal itself will continue.)

The current plan is to retire the MyUCDavis course tools in the spring quarter of 2010, but the date will change if needed, said SmartSite program manager Kirk Alexander. That decision and others will be guided by the SmartSite Oversight Committee created last spring. A pilot project to test the improved SmartSite Gradebook is presently due in spring 2009.

SmartSite, which starts its second year as a campuswide system this fall, runs on the Sakai open-source software developed and supported by a group of more than 100 colleges and universities. Information and Educational Technology installed version 2.5 of Sakai on July 19. The upgrade fixed bugs, improved the user interface, and realigned SmartSite with the Sakai code base to set the stage for future upgrades and patches.

During SmartSite's first academic year as a full system, faculty created more than 1,600 course sites, and about as many project sites, for research groups, academic intranets, student projects, discussion forums, and other collaborative uses.

But many faculty have not used SmartSite, so this summer three students in the ET Students program visited faculty advisers in several departments to propose SmartSite training sessions tailored to those particular areas. The students wanted to raise awareness of SmartSite among faculty who don't use it, or who don't take advantage of existing training sessions.

The outreach dovetails with plans by IET-Academic Technology Services to focus more of its SmartSite training in academic departments. ■

READ MORE:

For more about SmartSite, visit smartsite.ucdavis.edu. Read about July's training session for administrative staff, the ET students outreach, and other previous SmartSite news, in the TechNews archive at technews.ucdavis.edu. For more about the SmartSite Oversight Committee, visit vpiet.ucdavis.edu/smartsiteoversight.cfm. For training available this fall, go to iet.ucdavis.edu/help/smartsite_workshops.cfm.

CAMPUS TECH *Wrapup*

UCCSC + Security: Next June our campus will host the annual University of California Computing Services Conference, with a twist: for 2009 only it will be combined with the every-other-year UC Davis Security Symposium. The merged event, UCCSC-Focus on Security, will have features from both events, and should attract people from other UC campuses. Mark the dates—June 15-17, 2009—and look for updates as the year advances.

TechNews requests your attention: This past June, Information and Educational Technology improved its *TechNews* Web site, adding a featured story, "most read" list and better descriptions of the stories. *TechNews* posts news and information about campus technology, on subjects ranging from phishing scam warnings to information about DavisMail. Check out the site, or subscribe to the free weekly email update, at technews.ucdavis.edu.

Time to enter WarnMe contact information: The campus is asking staff, faculty and students to enter personal emergency contact information into the new UC Davis WarnMe emergency notification service database.

The campus installed WarnMe last February so it can send emergency messages to all or part of UC Davis, including the Sacramento campus and off-site locations, by email, telephone, cell phone, and text messaging. The system uses contact information supplied by students and employees. Employee work contacts are taken from the campus directory, but it's best to have several contact points because people could be anywhere when an emergency strikes. (Personal contact information will not be included in the official university online or printed directories.)

"It is important to keep your contact information up to date in the campus directory and in WarnMe," said Valerie Lucus, campus emergency/continuity manager. "In an emergency, we can't notify you if we don't know where you are."

Enter or update your personal emergency contact information at warnme.ucdavis.edu by using your UC Davis loginID and Kerberos password. (Employees can update their campus directory listings at listings.ucdavis.edu/update.) Read more at warnme.ucdavis.edu.

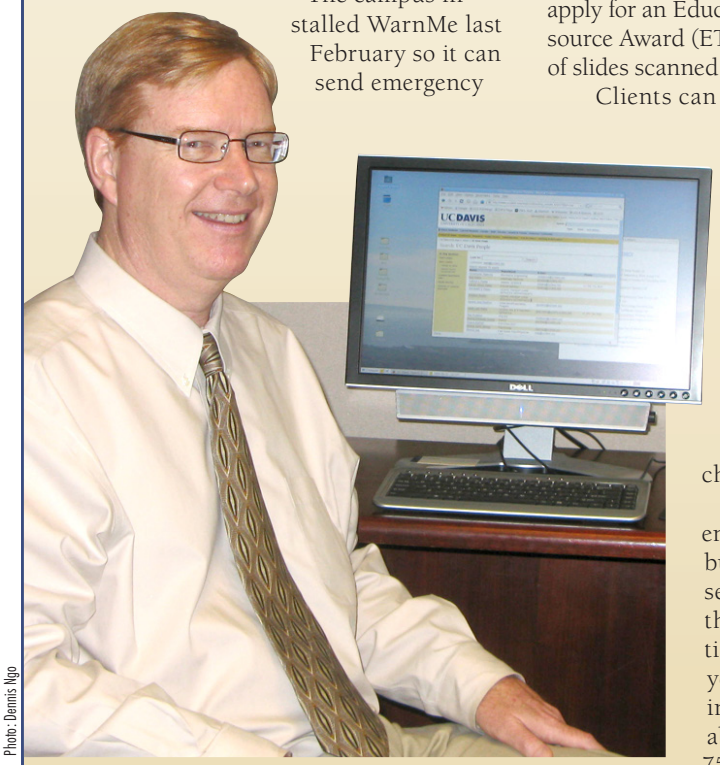

Photo: Dennis Ngo

New IT architect: David Walker started as campus information technology architect Aug. 4. Learn more about him, and his job, by searching the archives at technews.ucdavis.edu.

Slide scanning service now carries a fee: The Academic Technology Services department of Information and Educational Technology is now charging a fee for all slide-scanning services. Prior to this, faculty could apply for an Educational Technology Resource Award (ETRA) to get limited numbers of slides scanned for instructional purposes.

Clients can bring 35mm slides to Surge II to be digitized for various uses. A multimedia specialist scans the slides "and can do any enhancements if the client needs or wants them done," said Jennifer Radke, business manager for IET-Academic Technology Services. Clients, who are mostly faculty, will be charged per slide.

The campus considered ending the service due to budget constraints, but the service is widely used. More than 4,000 slides were digitized in 2007-08. To digitize your slides, visit IET-ATS in Surge II. To learn more about the service, call (530) 752-2133 or email ats@ucdavis.edu.

Free slide scanning without enhancements is still available on a self-serve basis from scanners in 1101 Hart Hall and Meyer Media Lab.

Useful, funny and honored: Leejay Abucayan graduated from technocultural studies in June. But he left behind a video podcast about computer security that judges in a national contest liked enough to honor twice this fall. The podcast, both useful and amusing, won "best of category" among promotional materials created by students, and an "award of excellence" in the promotional video/audio category from the Association for Computing Machinery Special Interest Group on University and College Computing Services (aka SIGUCCS). Judges called it a "benchmark entry for student-created podcasts."

Abucayan created the podcast for the Information and Events unit in Information and Educational Technology; undergraduate Phil Riley wrote the script. You can find it at iet.ucdavis.edu (click on "News & Pubs," then on "Cyber-Safety Basics" under "videos").

Judges also presented three awards of excellence to two other I&E projects this year: two for bus posters designed by Rich Wylie, also a June graduate, and one for the "UC Davis Cyber-safety Basics Tutorial" designed and written by communications analyst Julie McCall. The I&E unit has won 26 awards from SIGUCCS since 2000, including 12 since 2006.

Why your log-in looks a little different: Starting this fall, some widely used services at UC Davis are switching their authentication modules—a mechanism that helps faculty, staff and students access restricted applications and Web sites—from Distauth to the more reliable, secure, and faster CAS. Your campus log-in ID and password will not change. Most people will notice only that the log-in page—the mostly white screen that asks for your ID and password—looks a little different with CAS.

Several campus applications already use CAS, and all new applications developed in Information and Educational Technology (IET) will use it. This includes DavisMail (you can read more about that on Page 2).

Other changes started Sept. 19, when IET switched the authentication module for the MyUCDavis Web portal and course management tools to CAS. (Anyone who uses MyUCDavis to navigate to Geckomail and certain administrative applications, including Direct Deposit and MyTravel, might

Photo: Leslie Madsen-Brooks

Second Life at SITT: Milmon Harrison, a Chancellor's Fellow and associate professor in African/African American Studies, was one of the presenters at the yearly Summer Institute on Teaching and Technology, which met Sept. 8-12 this year. The themes for the daily labs and lectures were "Teaching Large Classes" and "Teaching With and for Networked Collaborators"—at his session, Harrison talked about how he taught with the virtual world Second Life. The institute will return in September 2009; learn more at trc.ucdavis.edu/trc/sitt.

have to authenticate twice until the authentication component for those services is switched to CAS.)

More migrations from Distauth to CAS are planned this fall for the campus online directory listings and MyInfoVault. The UC Davis WarnMe emergency notice system will use CAS from the start.

Eventually the Distauth modules will be retired, but they're widely used on campus, and a complete transition might take awhile. Owners of applications that use Distauth will determine their own timelines.

Until Distauth is gone, navigating between various UC Davis authenticated applications and Web sites will require dual authentication, if you're going from one that uses CAS to one that uses Distauth, or vice versa.

Direct questions to the IT Express Computing Services Help Desk, (530) 754-HELP (4357). To move a Distauth-protected service to CAS, please contact Hampton Sublett at hbsublett@ucdavis.edu.

One more thing: Log-in screens are also seeing one other change, although it's not caused by the switch from Distauth to CAS. Prompted by the phishing scams that have peppered UC Davis email users this year, the campus is adding a new security notice to the log-in page in both Distauth and CAS. It reminds people that they should use their computing account log-in ID and password only when authenticating to campus Web sites and online services.

It also says UC Davis will never ask anyone to confirm or verify their computing account by providing their password via telephone or email.

(While we're on the subject: for optimal security, shut the browser after you log out of a secure service.)

Read about the Roadmap: The newest IET Report has updates on 76 campus tech ventures, including major initiatives such as the Administrative Computing Policy and the Administrative IT Services Roadmap. Information and Educational Technology produces the report three times a year. To read the latest one, which covers June to September, go to iet.ucdavis.edu. Then click on "IET report" in the "News & Pubs" box. ■

Dial-up modems, most pay phones are exiting

A roundup of news involving the Communications Resources department of Information and Educational Technology in the latter half of 2008

Campus will end dial-up Internet access service: The campus will end its dial-up modem service, which provides off-campus access to the Internet and the UC Davis computing network, on Jan. 1, 2009.

The access has been free to faculty, staff and students since 1997, but demand has dwindled the last three years as former users switched to commercial Internet service providers that offer much faster connections. The reduction is part of IET's $1.46 million in budget cuts for 2008-09.

The modems retain enough capacity to satisfy demand expected through December, although users might get a busy signal during peak periods.

Alternatives include:

• DSL, cable modem, or another dial-up link, available from commercial Internet service providers.

• Cellular mobile data cards, a wireless alternative offered by various cell-phone carriers.

Phone bills switch to eBills: To trim paper use and save money, campus phone bills will now arrive electronically. The switch from paper began at the start of October, when subscribers were due to receive their eBills for August, September, and October. Telecommunications representatives from each campus department have been notified.

Each bill will contain slightly more information than previously, now that paper consumption is not a consideration. Otherwise, the bill will essentially be the same as before.

Most campus pay phones removed: The spread of cell phones had already made pay phones a rare sight on campus. Because of the tight budget, they're getting scarcer: Most of the last 38 will be replaced with courtesy phones by or during this fall.

The campus had more than 110 pay phones eight years ago. They once paid for themselves through usage fees. As cell phones became common, use of pay phones dropped, and the phones became an expense to the campus. Removing them saves money in a difficult budget year.

Some departments are keeping the pay phones in their buildings and will pay the cost. The rest will be replaced with courtesy phones that can connect with 911 and any campus number. ■

On the horizon, a 'very rewarding' project

Security (from page 1)

continue to improve. With a security program, you're never really done.

How do you keep up? The computing system here is complex, and used by people with vastly different needs, skills, and security habits. Online crime evolves. Tools improve. How do you focus?

We look at the threats and assess the risks. Our cyber-safety program has 16 security standards that all campus units must satisfy. Even with the 16, we identify which ones have higher priority. We can't address everything. We focus on the threats that pose the highest risk.

That's one way of helping to define where we go. The other part is working with campus units to help determine where to place our attention. Much of the computing and security at UC Davis is decentralized. Getting input from campus units on the threats and risks that people are seeing is vital, so we can determine how to move forward as a campus.

UC Davis also participates in national forums for security incidents. We receive and share information with other institutions of higher education.

What are the biggest current threats?

One would be the zero-day exploits. They occur when computer vulnerabilities are under attack and the vendor responsible for fixing the problem has been unable to release a corrective patch. A zero-day exploit could let a virus run wild or allow malicious traffic to enter the campus network. We've deployed network sensors to help us repel many serious zero-day attacks.

Another would be the phishing schemes that have been hitting campus. These email messages often appear to come from help desk or email administrators. They encourage the recipient to respond to a fictitious account problem by sending their campus account and password to another party's email address.

Despite our best efforts to inform campus account holders that UC Davis never requests account and password disclosure, some individuals still read the message, are concerned, and out of that concern respond to the phishing message. Unfortunately that's what the sender wanted, and then the sender harvests their account and password. The sender can then use the account to generate thousands of new spam or phishing messages, or some other bad use.

We try to identify campus email accounts that have responded to known phishing messages. One thing we struggle with is, once we find individuals who have responded to the messages, what do we do? Our records show only that they responded. We don't know how they responded.

Biggest current threats? One would be the zero-day exploits. Another would be the phishing schemes that have been hitting campus.

It matters whether they sent in their password, or told the sender to get lost.

Right. When an account holder has responded, the most effective security response is to disable the account from further use and ask the holder to reset his or her password. You can see the issue. If you disable the account of someone who provided their account and password, they're very thankful, perhaps. But if we disable an account from an individual who said 'get lost' to the message originator, they're not so pleased.

We're strengthening the campus security awareness program to emphasize that these phishing messages aren't always caught by the spam filters, and that the university never asks account holders to disclose their computing or email account and passwords.

Next: Managing IDs; maybe a forensics team

What are your goals for 2008-09?

Despite our budget constraints, we have a rather aggressive security program. One major project is working with the UC Davis Health System to develop and implement an identity management system. We're looking to help consolidate information about individuals' electronic identities—who they are, where they work, what roles and responsibilities they have.

To function, every application on campus needs these key components to some degree. Identity management systems can help gather and place that information in one location, so that every application on campus doesn't need to develop that same capability. Applications can then query the central identity management system and determine what the individual, or account holder, can do within the constraints of that application.

Right now, no one system will do that? The work is done by different systems?

Right. Several systems manage identity information. That adds security challenges, because it creates more identity-related systems to protect from unauthorized access.

But an identity management system would centralize that task, so people could work more easily across the campus network.

Yes.

We're at the beginning. The project's tasks, resources and budget are being defined. The project will bring new identity management tools to UC Davis and the Health System, and take several years to implement. It's extremely complex, but very rewarding to the university. It also offers significant benefits in cost reduction, security, and ease of use for campus units that develop applications.

Another program for 2008-09 is administering the cyber-safety policy. In September we released our annual cyber-safety survey.

That's where you ask people how they're doing in respect to meeting the cyber-safety security standards.

We ask through an online survey. After receiving the completed surveys, we prepare an analysis by each college, school and large administrative unit.

The survey helps colleges, schools and units to evaluate how well their security program has improved. It gives me information about campuswide security challenges, as well as common needs for security solutions. Finally, the survey information is used to report back to the chancellor and provost on the state of information security at UC Davis.

You're also working on a forensics project this year.

We're developing a proposal for a collaborative systemwide computer forensics program. Computer forensics can help us investigate security incidents and preserve the integrity of digital evidence.

We don't have quite enough workload for full-time staffing in this function. But systemwide, perhaps we could find enough work for up to two people full-time. So I'm collaborating with my security peers at the other UC campuses to develop a proposal for how UC Davis might develop this service, and offer it to other campuses, while providing some individual campus cost savings.

Done: Better off-site access, intruder-preventer

What were some big accomplishments last year in IT security?

One is the virtual private network (VPN) for electronic library references.

What's a virtual private network?

The term typically refers to a private network connection over a public network, such as the Internet. During fall 2007, a VPN was created to make it easier for UC Davis students, faculty and staff to remotely access library resources over the Internet.

The University Library licenses electronic content, such as research journals, that faculty or students need to access—sometimes from off campus. But the license holder for the content often restricts download access to requests from a campus IP [Internet protocol] address. If you're working from home or an Internet cafe, easily gaining that IP address is an immediate challenge.

We implemented a VPN that lets university affiliates use their Web browser, which just about everyone has on their home computer or laptop, to make a private connection over the Internet between their computer and the UC Davis network. This connection gives the end-user a campus IP address and, thus, access to the licensed material. To the electronic content provider, the end-user appears to make the content request from UC Davis. It's a tremendous benefit.

So if you can use a browser, know the library VPN's Web address, and have a campus computing account, that's all you need. Before, you had to reconfigure your browser on your remote computer [see more at www.lib.ucdavis.edu/ul/services/connect/vpn].

The project was a collaboration between IET and the University Library.

The campus also upgraded its network security alert system last year.

That was another major accomplishment. Previously, our security alert mechanism used intrusion-detection technology. It could report on intrusions, but had limits as to what it could do to prevent them.

The hardware for the detection system was nearing replacement age, so we upgraded the campus security alert system with intrusion-prevention sensors. They have been placed at critical points on the campus network, and can detect and terminate malicious traffic before it enters the network.

The gain seems obvious. You've gone from detecting an intrusion to preventing it.

The system can look at the traffic as it comes through, and if it meets certain criteria, block it at the campus border. Some UC medical centers use the same approach. It's expensive technology, but it affords us a tremendous advancement from where we were. We also identify malicious traffic as it leaves the campus, which can help alert a system administrator to a potential problem.

It's more than a technical job

Whom do you work with most on campus? Mostly technical people?

I communicate with technical staff, but my job is much broader than that. The security program requires an open communication channel to students, staff and faculty.

Students have received phishing messages, and we're stepping up our alerts to students about this threat. They have security responsibilities, as everyone does, in keeping their systems patched, and selecting a strong password. Staff and faculty have many computing systems, and those systems have maintenance issues as well.

I also work with the campus community to help move the campus security program forward. This collaboration often involves the Technology Infrastructure Forum [TIF], Campus Council for Information Technology [CCFIT], and Senior Advisors Group. The TIF consists of senior technologists from throughout campus. CCFIT, which has academic, administrative, graduate student and ASUCD representation, advises the provost, and the vice provost of IET, on technology use. The Senior Advisors Group has senior staff representatives from throughout UC Davis, and provides guidance to the chancellor and provost on administrative topics.

Members of the Academic Senate play an important role in the security program. For example, a cyber-safety oversight committee helps guide the direction of the campus cyber-safety policy and security standards. Professor Scott Stanley is the Academic Senate appointment to this committee. In addition, faculty members and researchers are consulted on measures to reduce security threats and risks.

One thing everyone should know

If you could tell every faculty member, employee and student one key message about campus IT security, what would it be?

That security is everyone's job.

It is not just the sole area of your technical staff member or IT help desk. Everyone has some role, whether it's applying patches, using anti-virus and keeping it up to date, selecting a reasonable password that can't be easily guessed or detected, or not responding to phishing messages. Everyone owns the security problem. That's the basic message.

For an idea what to do, visit the security Web pages [security.ucdavis.edu]. We have material on recommended security practices, plus instructional guides. They provide useful advice, for computers at home or at work.

We also give security software to campus technology users. Of particular note is the free Sophos AntiVirus software for campus and home use, software tools for whole-disk encryption, and software scanners that can identify electronic personal identity information stored on a disk.

A starting point would be the basic instructional guides.

Is there a No. 1 tactic, like 'have a good password'?

The tactical message is, no one security practice will protect you, unfortunately. You have to do a number of things to secure your computing system. A good password is key, but keeping your system up to date, and using up-to-date anti-virus, is equally important. We frequently find compromises from people who haven't patched vulnerabilities in their computing system. A password won't protect you against that problem.

Computer security practitioners call the need for multiple security layers a 'defense in depth' strategy.

So there's no one thing.

No one thing. ■

READ MORE:

Read more about campus IT security, including practical advice that will make your online life easier and safer, at security.ucdavis.edu.

Photo: Dennis Ngo

One person, six main areas

Bob Ono says his responsibilities as coordinator of IT security for UC Davis focus on six areas:

- Developing and implementing an information security program.
- Providing campus leadership on issues of security and privacy.
- Investigating security breaches. "The assistance from IET incident investigators may range from looking up attack origination information, analyzing log data or advising on physical security issues, to working with the campus police department."
- Communicating on security and privacy issues within UC Davis, and externally.
- Working with UC peers. "For example, UC San Diego performed some network scans for us, and we are developing a potential program for computer forensics that could support other UC campuses."
- Working with others in higher education.

Campus telecom starts building for the 2010s

The big job of installing the network described in UCDNet3, a six-year project to equip the campus telecom system for the data demands of the next decade, began in earnest this summer.

As the work progresses between now and 2014, people should notice that data is moving faster both to and from UC Davis, huge files are moving more easily, and the wireless network is growing. If the installations go smoothly, people on campus shouldn't notice disruptions—just better performance.

As the deployment progresses, the new network will move data 10 times faster than the existing network has.

By early fall, the Communications Resources section of Information and Educational Technology had:

• Installed part of the faster network core. "We're basically laying the groundwork for improving both the speed and the ability of the network to support converged services" such as videos and VoIP (telephone calls placed over the Internet), said Mark Redican, manager of the Network Operations Center and head of the UCDNet3 project.

• Started replacing the area distribution frames, which route network traffic to various large segments of the campus network. The department is doing this work outside of normal business hours and doesn't expect it to interrupt network service.

• Finished replacing the old access points on the campus wireless network with more capable equipment, to help support the wireless network's further expansion.

Decisions about where the wireless network should grow will be guided by the new Telecom Advisory Board chaired by Matt Bishop, a professor in the Department of Computer Science and a co-director of the Computer Security Laboratory. Redican and others expect to begin meeting with the board, whose members include faculty, research, staff and student representatives, in October.

Communications Resources wants to get the board's sense of priorities as to which buildings should get the expanded wireless and faster network connections first, Redican said. The work will occur in phases, and some parts of campus need the improvements sooner than others.

As the deployment progresses, the new network will move data 10 times faster than the existing network has. It will have more reliable electronics, better security, an improved ability to identify and prioritize network traffic, and increased wireless coverage and systems. The expanded capacity will support the fast transmission of huge data files needed to support advanced research, as well as high-definition video.

UCDNet3 received approval from campus leadership to proceed this year. It is the product of extensive planning, testing and review. ■

READ MORE:

For a complete story about UCDNet3, see "A faster, more wireless future" in the spring/summer 2008 IT Times (find the article in the archives at technews.ucdavis.edu). For technical and maintenance schedules and similar information about UCDNet3, visit ucdnet3.ucdavis.edu.

DVD, video checkout services will move from Hart Media Lab to Shields Library

Faculty and students who want to reserve or check out DVDs and videos for coursework will soon have a new destination: the Reserve Services Desk of Shields Library. The media reserve and checkout services in Hart Hall's Media Distribution Lab will move to Shields by summer 2009.

Hart Media Lab currently houses thousands of DVDs, VHS tapes, and non-print media for use in instruction, plus equipment to view them. Most customers are faculty who check out material to show in class, or students who come in to view videos.

Starting in summer 2009, many of the most heavily used titles in Hart Media Lab will be permanently transferred to the General Library, with access available through Reserve Services. The Information and Educational Technology computer lab in 163 Shields will have a few machines set aside for viewing the films. As part of the transition, many older VHS titles will be replaced with DVD versions.

The change means the Hart lab will gain space to install more open-access computers for general use, said Tim Leamy, computer lab manager for IET-Academic Technology Services.

During fiscal year 2008-09, the General Library and IET-ATS staff will prepare media titles for transfer to the Shields Library Reserves unit. As they are processed, the cataloged materials will be listed in Harvest, the Library Catalog (see more at www.lib.ucdavis.edu). The transition, a joint project between the library and IET, takes advantage of the strengths of each department.

"There will be a lot of behind-the-scenes work between now and next summer," Leamy said. More publicity about the move is planned. Older materials that have not been used recently, and are not likely to be used much in the future, will not be moved.

The permanent collection being transferred to the library is owned by the university. Titles are usually acquired through undergraduate academic grants (see trc.ucdavis.edu/TRC/grants/mini_travel.html), but can also be donated. ■

READ MORE:

For more on the transition, video checkout and reserve services, visit hartmedialab.ucdavis.edu/toshields.html.

IT Times

technews.ucdavis.edu

The ***IT Times*** is published by Information and Educational Technology. It's a free companion to ***TechNews***, an online source of campus tech news and information available at technews.ucdavis.edu.

IET staffers produce the stories in the ***IT Times*** unless otherwise noted. The articles may be reprinted if the source is quoted and credited accurately.

Layout by Tom Jurach. Items written by Bill Buchanan and Phil Riley. Buchanan is also the editor. Reach him at wrbuchanan@ucdavis.edu or (530) 754-5466 with ideas, comments, or questions.

UCDAVIS INFORMATION & EDUCATIONAL TECHNOLOGY

UCDAVIS CENTENNIAL