



<http://www.latimes.com/news/printedition/la-me-hacks30may30,0,659003.story?page=1%26coll=la-jobs-counselor-2002>
From the Los Angeles Times

College Door Ajar for Online Criminals

Hackers discover that universities are rich in personal data and easier prey than banks.

By Lynn Doan
Times Staff Writer

May 30, 2006

Computer systems at universities across the nation are becoming favorite targets of hackers, and rising numbers of security breaches have exposed the personal information of thousands of students, alumni, employees and even college applicants.

Since January, at least 845,000 people have had sensitive information jeopardized in 29 security failures at colleges nationwide. In these incidents, compiled by identity theft experts who monitor media reports, hackers have gained access to Social Security numbers and, in some cases, medical records.

"There are so many examples within the last year demonstrating that these universities are just real, true, vulnerable targets," said Michael C. Zweiback, an assistant U.S. attorney in Los Angeles who prosecutes hackers. "All of a sudden, it seemed like we were adding on another university every week to look into."

Although comprehensive statistics on breaches of college computer systems aren't collected by a single entity, industry experts agree that the situation is growing worse.

Computer security is an increasing concern for all types of private groups and government agencies. Last week, the Department of Veterans Affairs confirmed that electronic records of up to 26.5 million veterans and some spouses were stolen from the home of a federal employee.

Cyber security officials say hackers are realizing that colleges hold many of the same records as banks. But why hack a bank, one official asked, "when colleges are easier to get into?"

Colleges accounted for the largest percentage, roughly 30%, of computer security breaches reported in the media last year, according to ChoicePoint, a consumer data-collecting firm in Georgia.

FBI Special Agent Kenneth McGuire said that five years ago, his cyber crime unit in Los Angeles worked on one to three college hacking cases at a time. On a recent afternoon, his team was working with six colleges whose systems had been hacked.

Arif Alikhan, who oversees computer hacking cases for the U.S. attorney in Washington, said that when he was chief of cyber crime in Los Angeles between 2001 and 2005, his caseload doubled.

And for the first time in seven years, colleges identified security as the most critical issue facing their computer systems, according to a survey of about 600 colleges released this month by Educause, a nonprofit group that promotes information technology use. In a 2000 survey, security wasn't even among the top five concerns.

Hackers are drawn to colleges for various reasons.

In March, 41 Stanford University applicants hacked into the admissions system to see if they had been accepted. A man accused of hacking into USC's admissions system last year said he was only trying to prove that it was vulnerable.

In December, hackers appear to have broken into a system at the University of Washington to find a place to store their music files.

The openness that's rooted in the nature of academic institutions is partly to blame.

"Students want to be downloading MP3's. Professors want a system for general research," McGuire said. "Whenever you have such large portals to information open, you're going to have vulnerability to attacks."

Erich Kreidler, who teaches an engineering class at USC, said he posts everything online, including grades and final exams. "It's about convenience," he said.

But convenience can have a price.

Last month, the University of Texas discovered illegal access to 197,000 Social Security numbers of students, alumni and employees. Days later, a San Diego man was charged with hacking into the USC admissions system in June 2005.

Ohio University confirmed its third security breach since April, together compromising 360,000 personal records and a number of patented data and intellectual property files.

And Sacred Heart University in Connecticut reported last week that a security breach has compromised the Social Security numbers and some credit card numbers of 135,000 people — some of whom never applied to, worked at or attended the university.

Like many universities, a spokeswoman said, Sacred Heart collects personal information from college entrance exams, college fairs and recruiting firms. Robert M. Wood, chief information security officer at USC, said the college's computer system is scanned by hackers an estimated 500,000 times a day.

"It's pretty much a lot of doorknob rattling," he said. "But occasionally, they find an open door."

USC has reported two security breaches in the last year.

The University of California doesn't track security breaches, but ChoicePoint has logged five hacking incidents at UC campuses since January 2005. The California State University system reported at least 24 breaches since July 2003.

In March, an 18-year-old New Jersey man was convicted of breaking into a dozen systems at San Diego State. He was sentenced to three years' probation and must pay the school \$20,000 in restitution.

John Denune, technology security officer for San Diego State, said the 2003 hack exposed the Social Security numbers of more than 200,000 people. The hacker wiggled his way through an outdated system in the drama department to reach the financial aid system.

Targets of hacking have been obscure, such as 1,700-student Anderson College in South Carolina, and well-known, such as Notre Dame. Finding the money to pay for security

upgrades has been a major challenge for several schools.

"A university is fighting for every dollar to maintain a good education standard," said Rick Jones, an information security consultant in Los Angeles. "It doesn't necessarily allocate a security budget — at least not until it gets hit a couple times."

One identity theft protection firm in Arizona is catering to the college crowd. LifeLock, which charges consumers \$10 a month to protect personal data, ran a full-page newspaper advertisement after the recent University of Texas hack, targeting those affected.

"We told everyone, 'You have been victimized once by the university. Take steps today,' " said Todd Davis, chief executive of LifeLock.

LifeLock has also forged partnerships with the University of Oklahoma and Arizona State University and is in talks with two other institutions.

As hacks ensue, college officials have had no choice but to increase security.

San Diego State doubled its computer security staff after the disastrous hack of 2003, said Denune, the campus security chief.

"Increasing security is expensive, it's time-consuming, and unless someone really sees the threat, it's easily put aside," he said. "This was a wake-up call."

Other colleges now require students to download anti-virus and firewall software before connecting to campus systems.

At Purdue University in Indiana, which reported two security breaches last year and two this year, students must change their passwords monthly to access class schedules, grades and e-mail.

The efforts are part of SecurePurdue, a program the college launched a year ago to counter the rising attacks, said Steve Tally, IT spokesman for the university.

"Universities are very attractive to hackers," he said. "Purdue has a very good name internationally and, unfortunately, it's brought us the kind of attention we don't want."

In 2004, the college began phasing out the use of Social Security numbers to identify students and employees.

In response to last year's hack, USC has reprogrammed its admissions system and requires users to change their passwords more often.

A technical security department created three years ago routinely scans computers connected to USC's network looking for machines that aren't equipped with updated anti-virus software.

At some colleges, new security measures have sparked complaints from students inconvenienced by lengthy virus scans and password prompts. But others say too much security is better than too little.

Tyler Dolezal was one of the 197,000 individuals whose Social Security numbers had been exposed in April's breach at the University of Texas. Dolezal has spent the last month trying to place fraud alerts with credit reporting agencies — a process that turned out to be unexpectedly complex because Dolezal, 18, hasn't established credit.

"These college systems hold really sensitive information on a whole lot of people," Dolezal said. "That needs to be protected as much as possible."

*

(INFOBOX BELOW)

Computer hacking

Since January 2005, 15 universities in California have reported computer security breaches of personal records, affecting 614,080 individuals. Below is a sampling of those incidents:

Campus: USC

Individuals Affected: **270,000**

Incident: **July 8, 2005:** Hack to online application database exposes names, addresses and Social Security numbers of students.

*

Campus: UC Berkeley

Individuals Affected: **100,000**

Incident: **March 11, 2005:** Stolen computer compromises names and Social Security numbers of students and applicants.

*

Campus: Sonoma State

Individuals Affected: **61,709**

Incident: **Aug. 8, 2005:** Computer hack exposes names and Social Security numbers of all students, faculty, staff and applicants from 1995 to 2002.

*

Campus: Cal State Chico

Individuals Affected: **59,000**

Incident: **March 14, 2005:** Computer hack exposes names and Social Security numbers of current, former and prospective students, faculty and staff.

*

Campus: USC

Individuals Affected: **50,000**

Incident: **Nov. 11, 2005:** Stolen computer server compromises names, Social Security numbers and other personal information of employees, donors and patients of the Keck School of Medicine.

*

Campus: Cal Poly Pomona

Individuals Affected: **31,077**

Incident: **July 29, 2005:** Hack of two computer servers exposes names and Social Security numbers of current and former faculty, staff, students and applicants.

*

Campus: Stanford University

Individuals Affected: **10,000**

Incident: **May 11, 2005:** Computer network breach compromises Social Security numbers and other personal information of recruiters and students.

*

Campus: UC Davis

Individuals Affected: **50**

Incident: **April 3, 2006:** Stolen briefcases compromise names, addresses and Social Security numbers of health clients.

Sources: ChoicePoint, news reports

If you want other stories on this topic, search the Archives at latimes.com/archives.

TMSReprints
Article licensing and reprint options

Copyright 2006 Los Angeles Times | [Privacy Policy](#) | [Terms of Service](#)
[Home Delivery](#) | [Advertise](#) | [Archives](#) | [Contact](#) | [Site Map](#) | [Help](#)

PARTNERS:  