



InformationWeek

BUSINESS INNOVATION POWERED BY TECHNOLOGY

UCSF Break-In Puts Info On 46,000 At Risk

The University of California at San Francisco began notifying students, teachers, and staff that their names, Social Security numbers, and bank account numbers may have been accessed during a security breach.

By Sharon Gaudin, [InformationWeek](#)

April 5, 2007

URL: <http://www.informationweek.com/story/showArticle.jhtml?articleID=198800502>

Personal information for 46,000 students, faculty, and staff at the University of California at San Francisco is at risk after a hacker broke into the network, campus officials said this week.

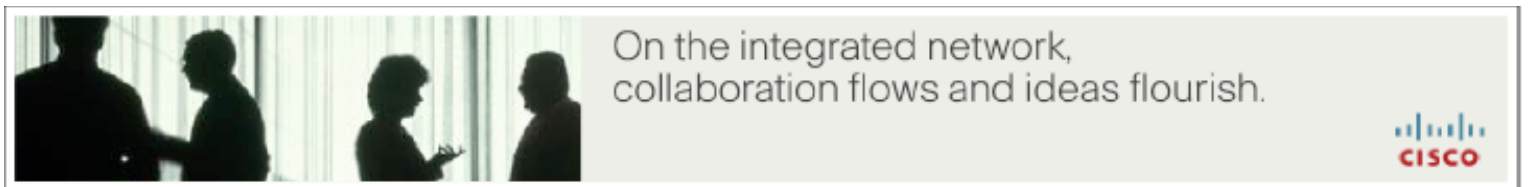
The university has sent out [advisories](#) that there was a security breach in a server on the school's network, and a hacker may have accessed their names, Social Security numbers, and bank account numbers. The university hasn't released any details about how the hacker accessed the server, which was located in the school's system-wide data center.

An advisory on the university's Web site noted that the compromised server was taken offline once the break-in was discovered in late March.

The school also advises anyone who thinks their accounts have been misused to contact the university's [police office](#) as well as credit agencies and their banks. For more information about the security breach and how to protect personal information, the university set up [this Web site](#).

The University of California isn't alone in its recent data loss. A stream of losses has made headlines in the past several months.

It was announced in February that a [laptop stolen from a secure office](#) at the Seton Family of Hospitals put identifying information on 7,800 patients without health insurance at risk. WellPoint, the country's largest managed care firm, had better luck. Last month, the company began informing customers that an unencrypted disc with the personal and health information of about 75,000 people had been lost. The [disc was found the next week](#).



Copyright © 2006 [CMP Media LLC](#)