THE UNIVERSITY OF TEXAS AT AUSTIN

Quick Links go

Data Theft and Identity Protection

| UT Directory | UT Offices A-Z | Campus & Parking Maps | UT Site Map | Calendars | UT Direct | UT Search | UTOPIA |

UT Home -> Data Theft Home -> Initial Report (March 5, 2003, 10:00 p.m.)

Data Theft Home

Data Theft Update (October 2003)

Latest Statement from the U.S. Attorney (March 14, 2003)

Initial Statement from the U.S. Attorney (March 6, 2003)

Initial Report (March 5, 2003, 10:00 p.m.)

Am I Affected?

What We Are Doing to Protect SSNs

ID Protection Resources

How To Contact Us

Español

(**Lea esta página en español.**)

Initial Report -- March 5, 2003, 10:00 p.m.

On Sunday, March 2 at 7:20 p.m., computer systems personnel at UT Austin discovered a computer malfunction. The affected computer system was immediately shut down, and detailed analysis was begun.

What happened?

The malfunction was assessed to be the result of a deliberate attack from the Internet. Subsequent analysis revealed that a security weakness in an administrative data reporting system was exploited by writing a program to input millions of Social Security numbers. Those SSNs that matched selected individuals in a UT database were captured, together with e-mail address, title, department name, department address, department phone number, and names/dates of employee training programs attended. It is important to note that no student grade or academic records, or personal health or insurance information was disclosed.

Is there evidence that the stolen data have been misused or disseminated?

UT, in conjunction with the U.S. Attorney's Office, the U.S. Secret Service, and other law enforcement agencies, has focused its efforts since Sunday evening on identifying the perpetrator(s) of the break-in and recapturing the stolen data. To date there is no evidence that the stolen data have been distributed beyond the computer(s) of the perpetrator(s).

What is UT doing about this?

UT's highest priority has been to identify the source of the attack and to cooperate with law enforcement authorities to capture the perpetrator(s), and any associated computers and data. Our second priority will be to assess the extent of further data exposure – if any – and to establish a proactive communication program with affected individuals and the UT community.

How many individual records were exposed?

Approximately 55,200 individuals had some of the above data exposed. This group includes current and former students, current and former faculty and staff, and job applicants.

How will affected individuals be notified?

The University is currently developing a communication plan and will contact affected individuals as soon as possible. At this juncture, there is no evidence that the data have been further exposed or misused.

To send a comment or question to the UT Incident Response Team, please e-mail **datatheft@its.utexas.edu** (do not send your Social Security number in any e-mail message).

UT regrets this incident and commits to do whatever is required to ensure the integrity of the data of all our past and present colleagues.

Daniel A. Updegrove
Vice President for Information Technology
The University of Texas at Austin

Updated 2003 April 24
To be contacted by the University, please complete the Web form.
For questions or comments, call the **DataTheft Hotline** at **475-9020** or toll-free at **(866) 657-9400**.
For privacy concerns read our privacy policy.