

---

[Jobs and internships for students - click here](#)

[Login](#) | [Register](#)

---

# SIUC hacked, more than 900 identities at risk

## Social Security numbers vulnerable after breach

By Ryan Voyles

[rvoyles@siu.edu](mailto:rvoyles@siu.edu)

**Published:** Wednesday, February 17, 2010

**Updated:** Wednesday, February 17, 2010

Meagan Lewis said she never expected a Scantron to cost her so much.

Lewis is just one of about 900 students whose identities are at risk after a breach in the SIUC computer system. She said there have been multiple attempts to open credit cards with her information since the breach happened in January but none have been successful.

Someone used a virus to hack into an older computer in the department of mathematics and obtained Social Security information from students who took a math course five years ago, said university spokesman Rod Sievers.

“Sometime in the last couple of weeks one of our computers got hit,” he said. “We’re trying our best to get in contact with everybody in that class.”

The breach was just one of 94 malware cases that have happened in the SIUC system since Jan. 4, according to an e-mail from Curt Wilson, SIUC’s network security officer, sent to school administrators. Of the 94 cases, this was one of the few involving sensitive information.

Lewis, one of those students in Math 113 five years ago, said SIUC police told her she

<http://www.RemoteStorageBackup.com>

was the only one to file a report at this time and only 12 other students have contacted the math department.

“There is no reason for me to still be in the system,” Lewis said. “The university should protect its students and it’s frustrating to think this was able to happen.”

Lewis said representatives from the math department told her the information was accessed from an e-mail containing the results of a Scantron test that was sent to her professor five years ago. The e-mail still existed in the system, she said.

Her information has been deleted from the system, but she said there was never a reason for it to be there in the first place.

“When I went to Illinois for two years, they used different identification than your Social Security numbers,” Lewis said.

Sievers said he was unsure of the university’s liabilities if any student reported financial loss.

Sievers said the university followed its policy, the Personal Information Protection Act, which requires the school to inform all those who could be affected by an information breach. He said e-mails and letters were sent, telling those who could be affected to check their account, place a fraud alert on the account and report to authorities any irregularities on their account.

While he does not know what the university will do to rectify the current situation, Chris Wiegman said there are steps that can be taken to prevent another incident.

Wiegman, a network support specialist in the aviation department, said it is important for computers – especially older ones – to be regularly updated through patches, or else it could easily be at risk.

“People can write codes so when you are opening something you think is a legitimate

Web site, another program can open up in the background which can start reading your hard drive,” he said. “It can copy things off your hard drive or what you’re actually typing, and start sending off that information wherever.”

Sievers said there are thousands of computers on campus to watch over, and that the IT Department does its best to keep watch over the servers. He said he did not know why the one computer in the department of mathematics was targeted.

Todd Sigler, director of the Department of Public Safety, said the investigation is ongoing and although there are a few active leads, he said he is not too optimistic they will lead to anything solid. He said the best way to approach these investigations is to track the stolen Social Security numbers for suspicious activities.

“You’ll start tracking the person’s name, information, and see if anything interesting pops up,” he said. “Opening of credit card accounts, transactions made in unusual places. Those things are what we need in this investigation.”

Sievers said despite the recent breach, the university is among the best in preventing security threats.

“This is fairly common; our university computers are always under attack,” he said. “I think we do a pretty good job here on campus of keeping the damage to a minimum.”

But Lewis sees it differently.

“It’s up to me to deal with this mess, and it seems like they should do more than send letters to students to fix it,” Lewis said.

Editor’s note: Lewis is a former page designer for the Daily Egyptian.

Ryan Voyles can be reached at 536-3311 ext. 259 or at [rvoyles@siu.edu](mailto:rvoyles@siu.edu).

**Recommended:** Articles that may interest you

<http://www.RemoteStorageBackup.com>

[Any student can build a hovercraft](#)

[University expects cuts next fiscal year](#)

[University donations down](#)

[Simon: 'Yes' to lieutenant governor, if asked](#)

[About](#)   [School of Journalism](#)   [MCMA](#)   [SIUC](#)

The *Daily Egyptian*, the student-run newspaper of SIUC, is committed to being a trusted source of information, commentary and public discourse while helping readers understand the issues affecting their lives.

The *DE* is published by the students of SIU Carbondale. Except during vacations and exam weeks, The *Daily Egyptian* print edition runs Monday through Friday during the fall and spring semesters and TWTh during the summer semester. The Pulse, a Carbondale Entertainment Guide, is no longer separate, it appears in the newspapers daily.

© 2010 Daily Egyptian

web1.collegepublisher.com/se/Daily\_Egyptian   Powered by  and 