



SECTIONS	TODAY'S PAPER	 MY SAVED	
NEWS ▶	METRO ▶		
ARTS ▶	BUSINESS ▶		
SPORTS ▶	OPINION ▶		
LIFESTYLE ▶	MAGAZINE ▶		
INSIDERS ▶	TODAY'S PAPER ▶		
LOTTERY ▶	OBITUARIES ▶		
GLOBE NORTH ▶	GLOBE SOUTH ▶		
GLOBE WEST ▶	TERROR AT THE MARATHON ▶		
68 BLOCKS ▶			

Metro

# Thieves breach BU pay system

## 10 workers have checks rerouted

By **Matt Rocheleau** | GLOBE STAFF | JANUARY 08, 2014

 ARTICLE	 COMMENTS
--	--

 PRINT  REPRINTS  E-MAIL  SHARE

Internet scammers stole monthly paychecks from 10 Boston University employees last month after obtaining the workers' user names and passwords and rerouting their direct-deposit payments, officials said.

Access to work-related accounts of another 68 university employees was obtained by an outside computer using suspicious Internet protocol addresses, but officials said they do not believe that sensitive information of those workers was compromised in the breach.

Campus officials said the FBI is investigating the case, along with similar cases reported recently at several other unspecified universities, according to BU's news website, [BU Today](#). No suspects have

been identified, said Detective Lieutenant Peter DiDomenica of the BU Police Department, which is aiding the federal investigation.

Officials did not say how much money was stolen. BU has reimbursed the affected employees, said campus spokesman Colin Riley.

Riley called the scam unfortunate, but said it was “an opportunity to remind everyone once again that there are people out there with bad intentions.”

“It’s easy to fall victim to these scams, so you have to be diligent and vigilant,” he said.

Authorities said they believe the BU employees were victims of a common scamming technique known as phishing, in which people are lured by fraudulent but real-looking e-mails, links, or websites and then persuaded to provide personal information.

BU said it temporarily shut down its electronic payroll system Jan. 2 after learning of the breach. Three days later, the service was restored for all but 510 employees, because those employees had changes made to their direct deposit information during December.

The university said it has notified those workers to confirm that they made those changes. Those accounts will remain disabled until the employees respond.

The university said it is analyzing e-mails sent to the affected employees to try to identify any phishing messages that may be connected to the case.

Quinn Shamblin, executive director of information security at the university, said the suspicious IP address that used the BU employee accounts were located in the United States and Africa.

“It is extremely common for people engaged in this kind of criminal activity to attempt to hide their location by routing their traffic through a variety of computers between them and the intended victim,” he said. “This means that the IP addresses we detect at the far end may have nothing whatsoever to do with the actual attacker.”

Officials warned against providing sensitive information, including user names or passwords, to any unsolicited requests, via e-mail, phone, mail or other means of communication.

Shamblin also urged BU employees to regularly check their bank accounts when they are expecting

Try brain training tested  
by dozens of researchers



lumosity

Start Training →

direct deposits.

*Matt Rocheleau can be reached at [matthew.rocheleau@globe.com](mailto:matthew.rocheleau@globe.com). Follow him on Twitter [@mrochele](https://twitter.com/mrochele).*

 PRINT  REPRINTS  E-MAIL  SHARE

 ARTICLE

 COMMENTS

## Learn more

[SUBSCRIBE](#) [BOSTON GLOBE INSIDERS](#) [REFER A FRIEND](#) [EPAPER EDITION](#)  
[NEWS IN EDUCATION](#)

### MY ACCOUNT

[LOGOUT](#)

 [MY SAVED LIST](#)

[MANAGE HOME DELIVERY](#)

### CONTACT

[HELP](#)

[FAQS](#)

[GLOBE NEWSROOM](#)

[ADVERTISE](#)

### SOCIAL

[FACEBOOK](#)

[TWITTER](#)

[GOOGLE+](#)

### MORE

[ARCHIVES](#)

[PRIVACY POLICY](#)

[TERMS OF SERVICE](#)

[TERMS OF PURCHASE](#)

[WORK HERE](#)

© 2014 BOSTON GLOBE MEDIA PARTNERS, LLC