



THE UNITED STATES ATTORNEY'S OFFICE
WESTERN DISTRICT *of* MISSOURI

[Home](#) » [News](#) » [Press Release](#)

NEWS



**Two mU graduates sentenced for college e-mail spam conspiracy;
must forfeit \$440,000 in cash, property**

**Millions of e-mail addresses illegally harvested from computers at
hundreds of universities**

FOR IMMEDIATE RELEASE

September 16, 2011

KANSAS CITY, Mo. – Beth Phillips, United States Attorney for the Western District of Missouri, announced that two Missouri men and their company were sentenced in federal court today for their role in a nationwide e-mail spamming scheme that victimized more than 2,000 colleges and universities, including the University of Missouri.

Amir Ahmad Shah, 30, his brother, Osmaan Ahmad Shah, 27, both of Ballwin, Mo., and their business, i2o, Inc., represented by company president Amir Shah, were sentenced by U.S. District Judge Howard F. Sachs to three years of probation, including three months of home detention and three months at a halfway house. The court also ordered the Shahs and i2o to forfeit to the government \$439,820 in cash and property.

“It was extremely helpful, in the investigation of such a highly technical case, for us to reach out to industry experts in both the public and private sectors for their input,” Phillips said. “Their collaboration and the excellent work of the FBI’s Regional Computer Forensic Lab were integral to this successful prosecution.” Phillips voiced appreciation for the assistance of professionals at Cisco, the IT department at the University of Missouri and other universities, and the Department of Defense – Office of Inspector General – Defense Criminal Investigative Service.

The forfeiture includes a total of \$78,980 in several bank accounts, two residential properties in St. Louis and Columbia (valued at a total of \$344,250), a 2001 BMW belonging to Amir Shah and a 2002 Lexus belonging to Osmaan Shah, and several Internet domain names. The Shahs also forfeited hundreds of computer and electronics items that were either purchased with proceeds of the scheme or were inventory marketed and sold through the scheme, including computers, digital cameras, more than 200 IPODs, 175 Brighter Image Teeth Whitening Kits, and numerous other items.

On July 28, 2010, the Shahs both pleaded guilty to creating a spam e-mail scheme that targeted college students across the United States. They developed individualized e-mail extracting programs which they used to harvest student e-mail addresses from the University of Missouri and hundreds of other universities and colleges. They then used this database of more than 8 million e-mail addresses to send unsolicited

commercial e-mails selling various products and services (such as such as digital cameras, MP3 players, magazine subscriptions, spring break travel offers, pepper spray and teeth whiteners) to those college students.

From Jan. 1, 2004, to Feb. 28, 2005, the Shahs and their co-conspirators were successful in sending e-mails that were not caught by university and college spam e-mail filters by using a variety of methods. They set up hosting in China, which they called "Offshore Bullet Proof Hosting," meaning it was immune to complaints from recipients of their e-mails and provided them anonymity as to the origins of their e-mails. They bought and sold open proxies (computer servers that enabled them to make indirect network connections to other computers in order to camouflage the original source of their e-mail). They used bulk e-mail software to falsify e-mail header information and rotate subject line entries, reply-to addresses, and message body content in their messages. They also provided false information when registering some of their domain names.

The Shahs also admitted that they initiated their spam campaigns by using the bandwidth provided by the University of Missouri's computer network, thereby causing damage to the network and its users. Osmaan Shah, who was a student at the University of Missouri, connected to the Internet via the campus wireless Internet service and also connected directly to the network through an ethernet cable connection in a classroom or other campus building. The university's network sustained damage from the large amount of network resources and bandwidth used during the transmission of millions of spam e-mail through its system.

Co-defendant Paul Zucker, 58, of Wayne, New Jersey, also pleaded guilty to his role in the conspiracy and was sentenced to three years of probation and ordered to pay \$7,562 in restitution. Zucker admitted that he provided proxies, which were intended to be used both inside and outside of the United States for the purpose of sending spam e-mail messages. Zucker also admitted that he provided bulk e-mail software that was designed to falsify e-mail header information and rotate subject line entries, reply-to addresses, message body content, and URLs in their messages. This allowed conspirators to penetrate university and college spam e-mail filters.

In addition to the conspiracy, the Shahs and i2o also pleaded guilty to one count of aiding and abetting each other to access a protected computer without authorization and transmit multiple commercial e-mails with the intent to deceive or mislead the recipients (or any Internet access service) about the origin of those messages.

CAN-SPAM Act

In 2003, Congress passed the CAN-SPAM (Controlling the Assault of Non-Solicited Pornography and Marketing) Act, making fraud in connection with electronic mail a federal crime. Spam refers to unsolicited bulk commercial e-mail. Under federal law, it is illegal to send multiple commercial e-mails if the sender accesses a computer system without authorization, transmits the e-mails in such a way as to hide their origin, or materially falsifies the header information in the messages.

This case was prosecuted by Assistant U.S. Attorney Matthew P. Wolesky. It was investigated by the Federal Bureau of Investigation.