Florida man pleads guilty to role in cybercriminal exchange (Update)

August 18 2015, byJoe Mandak

A Florida man pleaded guilty to being part of a team that corrupted computer networks and sent millions of spam messages to people in order to help computer marketers collect email addresses and phone numbers.

Naveed Ahmed, 27, of Tampa, is a systems administrator and master's degree student at the University of South Florida. But from September 2011 to February 2013, he and two others earned between $2,000 to $3,000 weekly by conspiring to violate the Controlling the Assault of Non-Solicited Pornography and Marketing, or federal CAN-SPAM, Act of 2003.

The law is designed to protect people from receiving spam emails or text messages that contain either marketing or pornography.

Ahmed is one of 12 people federally charged for marketing their skills on Darkcode.com, a cybercriminal marketplace disabled by the FBI last month. A total of 70 people in the U.S. and 19 other countries were targeted in that takedown.

Ahmed faces up to three years in prison when he's sentenced Nov. 24 before Senior U.S. District Judge Maurice Cohill Jr. who accepted Ahmed's guilty plea to a single conspiracy count on Tuesday.

Assistant U.S. Attorney Jimmy Kitchen told the judge that Ahmed was part of a three-person team who used software to infiltrate computer and

cellphone networks with millions of users.

"I wanted to take responsibility because I know my actions were wrong," Ahmed told the judge. He and his defense attorney declined comment after the plea hearing.

One scheme involved using two China-based computer servers to scan and infect computer routers, mostly in developing countries. Ahmed and the others then anonymously sent spam emails to computers linked to the routers.

The other scheme involved a computer program Ahmed wrote that enabled the trio to generate random lists of cellphone numbers and correctly link them to the correct wireless networks that issued them. That enabled the trio to send spam text messages to those phones, also anonymously.

Both types of spam included Internet links that recipients could click on. Those who received the text messages were told they had won Best Buy gift cards that could be accessed by clicking the links.

Instead, computer and phone users who clicked the links were sent to Web pages controlled by Internet Cost Per Action networks, which are companies that gather email addresses and other personal information. Such companies are legal, but the means Ahmed and the others used to drive traffic to the companies' websites was not, Kitchen said.

The network paid Ahmed and the others for each email address they gathered. That money was sent though a Swiss bank account controlled by an unindicted—and so far unidentified—co-conspirator, who kept 10 percent for laundering the money, Kitchen told the judge.

Ahmed remains free on bond and can't use a computer unless it's

monitored by the government.

Defense attorney Melvin Vatz told the judge that Ahmed "may lose his job and his education" if he's forced to tell USF officials about his conviction. But Kitchen said that's the only way the government will be able to monitor Ahmed's computer use.

A University of South Florida spokeswoman confirmed Ahmed is an employee at the school and said his card and system access to buildings has been terminated.

Lara Wade-Martinez said USF is reviewing his eligibility to return as a student this fall.