

6 September 2008

By: Denisa Ilascu, Internet / SEO News Editor



11 men were charged with criminal counts for hacking into the wireless networks of several companies
thebiographychannel

Biggest Identity Theft Criminal Ring Charged

With several counts

Eleven people that are believed to have conspired in the largest hack and identity theft in history had been charged. According to the authorities, some of the numerous counts the men were charged with are conspiracy, computer intrusion, fraud and identity theft. The nationality of ten out of the 11 defendants has been revealed: three are from the US, another three from Ukraine, two are Chinese citizens, one is from Estonia and one from Belarus. The citizenship of the 11th remains a mystery, as everything authorities could find out about him was his online nickname. The criminals hacked into the wireless connections of major American retailers and, by using malicious software, managed to get credit card information of the customers of the affected stores. TJX Companies, BJ's Wholesale Club, OfficeMax, Boston Market, Barnes & Noble, Sports Authority, Forever 21 and DSW are only some of the companies that fell victim to the alleged criminals. After obtaining the valuable information, they either sold it to Eastern European hackers or used it to produce fake cards that were further on employed to withdraw important amounts of money from ATMs. To avoid tracking, the criminal ring used anonymous Internet-based currencies and placed their money in Eastern European bank accounts. "Computer hacking and identity theft pose serious risks to our commercial, personal and financial security," said U.S. Attorney for the Eastern District of New York Benton J. Campbell. "Hackers who reach into our country from abroad will find no refuge from the reach of U.S. criminal justice." Indeed, the penalty that the 11 face is harsh - in case they are found guilty for all counts, they will spend their whole life behind bars.

"While technology has made our lives much easier it has also created new vulnerabilities. This case clearly shows how strokes on a keyboard with a criminal purpose can have costly results. Consumers, companies and governments from around the world must further develop ways to protect our sensitive personal and business information and detect those, whether here or abroad, that conspire to exploit technology for criminal gain," said U.S. Attorney Michael J. Sullivan.