Schools Spawning A Breed of Hackers

By [The Moscow Times](#)

October 07, 2010

The U.S. Department of Justice said it may have been the most sophisticated computer fraud ever. For Viktor Pleshchuk, it was the chance to buy a brand new BMW and an apartment in his hometown of St. Petersburg.

The 29-year-old last month pleaded guilty to participating in a worldwide hacking scheme that led to the illegal withdrawal of more than $9 million from cash machines worldwide operated by RBS WorldPay, the U.S. payment-processing division of Britain's Royal Bank of Scotland Group.

The conviction shed light on a growing trend from Russia. Just as President Dmitry Medvedev seeks to persuade investors that his country is a safe place, more technology graduates are turning to cybercrime. The FBI last week charged 37 suspects from Russia, Ukraine and other Eastern European countries of using a computer virus to hack into U.S. bank accounts.

"The number of hackers reflects how many good engineers we potentially have in this country," Vladimir Dolgov, president of Google in Russia, said in an interview.

Russians committed more than 17,500 computer-related crimes last year, or 25 percent more than in 2008, according to the Interior Ministry's latest statistics.

'Childish Prank'

While cybercrime is proliferating, Russian laws against it were written in 1998, when hacking was often perceived as a "childish prank," Boris Miroshnikov, head of the ministry's anti-cybercrime department, said in a report posted on the agency's web site.

A ministry spokeswoman said the department has advised Russian lawmakers to impose stiffer penalties on hackers. She declined to be identified, citing department policy.

"We are working on that, but so far we haven't moved beyond discussions," she said.

Businesses around the world lose more than $1 trillion in intellectual property because data theft and cybercrime annually, according to a January 2009 report by McAfee, a technology security company based in Santa Clara, California.

Seeking to thwart the attacks, U.S. legislators in March proposed to use trade restrictions to penalize countries that provide safe haven to hackers.

Growing Threat

"The cybercrime threat coming from Russia is significant and growing," U.S. Senator Kirsten Gillibrand, a New York Democrat who supports the measure, said in an e-mailed response to questions. "It threatens America and undermines the Russians. It is in the best interest of both countries to find a way to cooperate and better control cybercrime."

The FBI said last month that the suspects from Eastern Europe stand accused on trying to hack into U.S. bank accounts to steal more than $3 million. In August, French authorities arrested a resident of Moscow who used his Internet network called CarderPlanet to sell stolen credit cards, the U.S. Secret Service said in a statement on its web site.

"This network has been repeatedly linked to nearly every major intrusion of financial information reported to the international law enforcement community," the agency said in the statement.

The government in Moscow needs to create jobs to help thwart cyber criminals. Their numbers have swelled since the collapse of the Soviet Union, when scores of Russian computer engineers turned to online crime, said Dmitry Zakharov, a spokesman at the Russian Association of Electronic Communications, a trade group that promotes Internet security in Russia.

"Hackers are not gangsters with knives, but young and talented kids from suburbs who don't have any other options to make a living," Zakharov said. "If the government will create jobs for them, many will follow the lead."

Shy Hacker

Medvedev, 45, who has a [video blog](#) and a [Twitter account](#), has said he wants to stop the

Russian brain drain and turn the economy away from energy exports toward one based on technology.

The president asked billionaire Viktor Vekselberg in March to oversee plans to create a hub for the development and marketing of new technologies in the Moscow suburb of Skolkovo, where tax breaks and other incentives would be offered to lure investment. Companies including Siemens, Cisco Systems and Nokia have agreed to participate in the project.

Pleshchuk was a "positive and shy" student who "worked hard," Sergei Sharangovich, head of the department that educated him, said in a statement on the web site of Tomsk State University of Control Systems and Radio Electronics.

After graduating, Pleshchuk moved to St. Petersburg and opened an e-commerce company before he got in touch with a group of international hackers who asked him to help crack WorldPay's database, Russian investigators said.

'Sophisticated'

The U.S. Justice Department last year indicted Pleshchuk and seven other hackers in Russia and elsewhere in Eastern Europe, saying on its web site that the group stole the data encryption that was used by RBS WorldPay to protect debit cards.

The cards were used to withdraw money from 2,100 cash machines in 280 cities in less than 12 hours, in what U.S. prosecutors called "perhaps the most sophisticated and organized computer-fraud attack ever conducted."

"We take fraud extremely seriously and have stringent security processes in place to protect our customers, which we

constantly review," Michael Strachan, a spokesman at RBS in London, said in an e-mailed statement.

Pleshchuk got a reduced sentence, including four years' probation, after he agreed to provide information about his accomplices, his lawyer, Yury Novolodsky, said in an interview in St. Petersburg last month. He was ordered to give up his assets, including the BMW and the apartment, to help pay the $9 million back to WorldPay.

"On the one hand, it's flattering," Sharangovich at Tomsk University said. "On the other hand, Pleshchuk didn't apply his knowledge the right way."

Original url:
https://www.themoscowtimes.com/2010/10/07/schools-spawning-a-breed-of-hackers-a2024