Cybercrime is world's most dangerous criminal threat

September 17 2010, by Adrian Addison

A crime epidemic is silently sweeping the globe as criminals turn our ever-increasing dependence on computers against us, and even the head of Interpol is not immune.

On Friday 300 of the world's top law enforcement officials concluded the first ever international police anti-cybercrime conference, facing the stark and growing threat from an estimated 105-billion-dollar illegal business.

And Ronald K. Noble, secretary general of the international police agency Interpol, told the cream of law enforcement from 56 countries that his identity had been "stolen" to create two Facebook profiles.

One of the impersonators used the fake profile to obtain information on fugitives targeted in a recent Interpol-led operation seeking on-the-run criminals convicted of serious offences, including rape and murder.

"Cybercrime is emerging as a very concrete threat," he said at the opening ceremony of the first Interpol Information Security Conference at Hong Kong's police headquarters on Wednesday.

"Considering the anonymity of cyberspace, it may in fact be one of the most dangerous criminal threats we will ever face."

And terrorists could also inflict a significant blow with a cyberattack on a nation's infrastructure, he added.

"Just imagine the dramatic consequences of an attack, let's say, on a country's [electricity grid](#) or banking system," he said.

"We have been lucky so far that terrorists did not -- at least successfully or at least of which we are aware -- launch cyberattacks.

"One may wonder if this is a matter of style. Terrorists may prefer the mass media coverage of destroyed commuter trains, buildings brought down, to the anonymous collapse of the banking system. But until when?"

The scale of the problem was also highlighted at the Asia launch of a new report, also in Hong Kong, on Thursday by Internet security firm Symantec.

Almost two thirds of all adult web users globally have fallen victim to some sort of cybercrime, the 2011 Norton Cybercrime Report: The Human Impact study says, from spam email scams to having their credit card details stolen.

China had the most cybercrime victims, at 83 percent of web users, followed by India and Brazil, at 76 percent each, and then the US, at 73 percent.

The study, of over 7,000 Internet users, also found that 80 percent of people believed the perpetrators would never be brought to justice. Fewer than half ever bother to report the crime to police.

Stacey Wu, a Symantec senior director, told AFP that just one of the firm's offices -- in Chengdu, China -- alone detects 100,000 cybercrime threats every single day.

"It is no longer just high school kids in their bedrooms sending out

malicious emails," she said. "It's organised criminals.

"They carry out silent, hit-and-run attacks that steal relatively small amounts of 20 dollars or so from 20 or 30 people. Then they move on."

Cybercriminals also trade in data stolen, often unnoticed, from a victim's computer. Credit card details, for instance, are sold on the black market for between five and 20 dollars.

"Identity and personal information theft is a big problem," Wu told AFP. "For example, if the criminal knows a person makes a lot of transactions online, the value of that person's information can be worth a lot more."

Cybercrime is worth an estimated 105 billion dollars, according to rival computer security firm McAfee, and US police say cybercriminals can earn around 23,000 dollars a week.

The biggest problem, and the criminal's greatest advantage, is complacency, says Professor Joseph Kee-Yin Ng, treasurer of the Internet Society Hong Kong.

"It is hugely important for people and companies to protect themselves," he told AFP. "The criminal is as real as any thief or mugger, you just can't see them."

(c) 2010 AFP