Syndicate hacks into firms' systems

RM1 MILLION: 11 arrested in Kuala Lumpur, Selangor, Pahang and Kelantan

FAREZZA HANUM RASHID AND ALIZA SHAH
KUALA LUMPUR
news@nst.com.my

MALAYSIA'S cybersecurity, though at a high level, is vulnerable to hacking.

This is evidenced by the arrests last month of 11 members of a syndicate that hacked into online purchasing systems using fake credit cards and raked in RM1 million.

The 11 members, comprising nine men and two women, were picked up here, Selangor, Pahang and Kelantan during Op Helang 3/16, a three-day operation that kicked off on April 25.

Commercial Crime Investigation Department (Multimedia and Cyber Crime Investigation) deputy director Senior Assistant Commissioner Mohd Kamarudin Din Md Din said investigations revealed that the members had been active since September.

He said police seized computers and telephones believed to have been used in the syndicate's cheating activities, and goods that were fraudulently purchased, to facilitate investigations.

Kamarudin said the modus operandi of the syndicate saw it using the data of fake credit cards to pay for products bought.

"When the transactions fail, they use an application that intercepts the backhand codings showing 'failed' and changes them to 'successful'.

"Upon receiving the 'successful' transactions, the suppliers will deliver the products to the buyer, not knowing the transactions were invalid," he said, adding that the syndicate also used fake or non-existent addresses to receive the products it had bought.

When the courier failed to deliver the packages to a location, it was instructed to go to another location fixed by the syndicate, said Kamarudin.

He said upon receiving the products, the syndicate advertised them in websites and social media to reap the profits.

"Its modus operandi was to buy products online using fake credit cards and resell them at cut-rate prices on other websites, including smart applications."

He said the syndicate targeted popular companies offering electronic goods, cosmetics, computer games and instant food.

During their crackdown on the syndicate, police confiscated computers, telephones and fake credit and debit cards.

Items ordered from the online shops, worth more than RM30,000, were also confiscated during their raid.

The 11 suspects have been remanded to facilitate investigations under Section 5 of the Computer Crimes Act 1997, which cites it being an offence for any act involving the modification of contents of any computer.

If found guilty, the suspects are liable to face a fine not exceeding RM100,000 or a jail term not exceeding seven years, or both.

"These arrests have proven police expertise and ability regarding the latest forms of crimes, which are more complex.

"We take this matter seriously and will not compromise with any party involved or planning to be involved in this activity."

Universiti Kebangsaan Malaysia (UKM) cybersecurity unit head Professor Dr Zarina Shukur urged consumers to be cautious when buying items from dubious online stores.

She said this latest scam, involving shopping portals, had raised the alarm bells for the public to be more vigilant while shopping online.

"If we compare the number of daily online scams with the number of daily transactions, I'm sure the number is not that big.

"However, it does happen and in most cases, it is because of the weaknesses of customers.

"Social engineering of online scammers is popular because it is much easier as compared with back-end coding or malware planted in the website," she told the *New Straits Times*.

Online shoppers, Zarina said, should make sure the online stores they visited were genuine.

"In general, online shopping is safe. However, we must take precautions."

Zarina said that online payment normally consisted of two parts: online shopping website and payment method.

She urged consumers to make sure the website was reliable, and to confirm the "URL" of the site as well.

She said consumers should ensure that the payment method could be trusted.

She advised consumers to use their personal computer and not a public computer or public wireless line.

"It is better if the websites have a 'Malaysia Trustmark' certificate," she said, adding that consumers could also look at the "zero liability policy" by credit card companies, which sees consumers not being held responsible for fraudulent charges.

Another UKM cybersecurity expert, Mohd Rosmadi Mokhtar, said there had been an increase in the number of hacking scams.