

Gullible Malaysians

By Sonia Ramachandran
and Tan Choe Choe
news@nst.com.my

KUALA LUMPUR: There have been many awareness campaigns and reports on cheating cases in the media. But these have done absolutely nothing to enlighten a gullible public.

Police are worried and bewil-

dered over a spike in the number of victims who have lost millions of ringgit to conmen.

What is of even greater concern are new methods employed by fraudsters, including "parcel" scams via social networking sites.

Those duped come from all racial and social backgrounds, age, as well as gender.

Commercial Crime Investigation Department (Cyber and

Multimedia Investigation Division) assistant director Assistant Commissioner Mohd Kamarudin Md Din told the *New Sunday Times* that victims suffered losses amounting to RM5 million via scams conducted over social networking sites last year, and RM2 million in 2008.

Cybercrimes such as "phishing" and "spoofing" are also on the rise.

Malaysians lost RM9.9 million to conmen last year in "magical" scams, said Assistant Commissioner Latt Mazura Mansor, the federal Commercial Crime Investigation Department (Corporate Investigation Division) assistant director.

There was an 80 per cent increase in such cases last year from 2008.

Victims thought they were get-

ting a miracle cure or magical solution to their problems or ailments.

"Some victims were told they were possessed by a spirit and had to be treated immediately," said Latt.

Police advise the people to cultivate a "verifying" culture. Malaysians, they said, were just too trusting.

REPORTS ON P6

6 NEWS

Thwarting cyber smooth criminals

By Sonia Ramachandran
sonia@nst.com.my

KUALA LUMPUR: Have you found your beau through a social networking site and he wants to send you a gift via courier? Beware, for you might end up being a victim of smooth cyber con artists.

The authorities are concerned over the spike in what they call "parcel" scams, which has caused victims to suffer millions of ringgit in losses. Cybercrimes such as "phishing" and "spoofing" are also on the rise.

The Commercial Crime Investigation Department's Cyber and Multimedia Investigation Division assistant director ACP Mohd Kamarudin Md Din said there were 120 "parcel" scam cases in 2008 involving losses of RM2 million, and the number rose to 345 cases involving RM5 million losses last year.

He said the modus operandi was similar in most cases with victims befriending the fraudsters through social networking sites.

"The fraudsters would say they are sending a parcel as a wedding present or as a gesture of friendship, or say they want to send money to buy property. The victim will then get a call from a 'courier company' seeking to verify his or her identity.

"Another call will come later saying the parcel has been retained by the Customs De-



ACP Mohd Kamarudin Md Din says people should check and verify everything

partment because of its contents, and that an 'anti-terrorist fee' has to be paid before it can be released. A bank account number will be given for the money to be banked in.

"Amazingly, some people fall for it and bank in the money," said Kamarudin.

He said "spoofing" was also on the rise. This is where fraudsters pretend to be bank officers, the police or other parties when making calls.

For 2008, said Kamarudin, there were 21 such scams reported to the police involving losses of RM128,000.

Last year, the number increased by more than 1,500 per cent with 333 cases involving losses of RM4.3 million.

"They are advanced now,



Internet fraudsters are using advanced methods to convince their victims.

The phone numbers that appear on the phones of victims are really those from a bank, police or a certain organisation. They use Internet features to spoof the number so when the victim receives the call, he would think it was the real deal.

"The fraudsters subscribe to Internet sites that sell spoofing features. There is even one country that legalises spoofing. This is the Internet so how can you stop this?"

He said one woman lost RM1.2 million through this method. She was told she had won a lottery through the phone and was asked to pay

"processing fees".

After she had paid up, they asked for more.

"They would tell you that you would lose everything if you don't pay up. This goes on until the victim becomes bankrupt."

Sometimes, he said, the fraudsters would call pretending to be from a bank.

"They would say that your identity has been used to subscribe for a credit card and there was a huge sum owing, or the credit card had been used for illegal purchases.

"The fraudsters would then offer to help settle the matter. They will connect you to the

'Central Bank' and to their 'Credit Card Fraud Unit' which does not exist.

"Someone from that so-called unit would ask you to follow their instructions which would include asking you to go to the ATM and enter certain numbers. In fact, you are transferring your money out.

"Sometimes they would threaten to freeze the account and ask the victims to transfer their money out immediately into a 'safe account' until the problem is solved," said Kamarudin.

The fraudsters, he said, would even pretend to be police officers.

"They would call and say they had received calls from another country notifying them that the victim's name had been used by a syndicate in that country. They would then say they are going to freeze the victim's account."

He said that people should check and verify everything.

"Accounts cannot be frozen through one phone call. If the bank wants to freeze your account, they will not tell you.

"And why would they help you transfer your money out of the account before it is frozen? Why freeze an empty account?"

Those falling prey to this are from all walks of life, including professionals and businessmen.

"I'm worried about this. We have had discussions with telcos to warn their subscribers of these scams. We are also trying to trace the owners of these 'safe accounts' and have managed to nab a few.

"These people are called cash mules. Malaysians lend their accounts to foreigners in return for a sum of money.

"They should be aware that what they are doing is illegal and they can be held responsible if their account is used for fraudulent purposes."

Another scam on the rise, he said, was phishing, where victims received emails from "banks" asking them to update their accounts.

"There are those who do so and their information will go to the syndicate and their money transferred out through Internet banking."

He said the public must be made aware that banks would not communicate with them via email.

"The link they are asked to click on is not genuine."

In 2008, there were 150 phishing cases reported involving RM464,000 in losses. Last year, there were 236 cases involving losses of RM1.6 million.

"We believe these three types of scams are being carried out by international syndicates working with locals."

What do you think?
Let us know at
nsunt@nst.com.my

NEW SUNDAY TIMES, FEBRUARY 21, 2010