


Sun, May 3 2009 - If you think there is nothing wrong with receiving unsolicited calls, text messages or e-mails, think again. Someone in possession of your name, contact number and place of work may be able to steal your identity.

Chia Wing Fei, the security response manager of F-Secure Security Labs, says that with this baseline information, someone could easily gather more particulars.

There are a few ways of doing this passive information reconnaissance over the Internet, pretexting or phishing, he says.

Pretexting is a form of social engineering where, for example, someone calls on the pretext they are from a financial institution regarding some suspicious credit card activity and requires you to verify or give additional data.

Once the full identity of the target is obtained, they may apply for new credit cards under your name and change the billing address so you will never receive the statements, says Chia.



Sonya Liew of the human rights committee of the Malaysian Bar Council says that typically, information about a person's movements and habits is being collected via electronic means every single day.

From the time you turn on your handphone, telcos can track where you are; when you pump fuel and use a loyalty card, petrol companies know who you are; if you pay with a credit card, the company knows where and how regularly you pump petrol. At work, your employer has your details, and when you park your car, you are being monitored via CCTV.

In today's age of computers, it is easy to collect and keep information and there are many people willing to sell this information. At the same time, people can use this information, piece it together and create a social profile of you.

We have come to a point where it is very easy to be a victim of identity theft, and it is becoming more rampant, says Liew, adding that Malaysians have to wake up and realise that people are making money from their personal details.

A private investigator (PI), who declined to be named, says that 75% of fraud happens because of insider collusion.

Today, with insider help, people can do anything they want, he says.

The PI says he has investigated cases where car loans and phone lines were registered under people who did not request for them.

Chia says there is no sure way of preventing one's details from being passed around.

You should be alert and aware at all times. There is usually something wrong if it sounds too good to be true, he says.

Bank Negara reported that it received a total of 165 complaints on unauthorised withdrawals last year. In most cases, victims of unauthorised withdrawals received an unidentified sms (from fraudsters) to inform them that they had won a cash prize.

The victims would then furnish the fraudster with all other details, leaving the fraudster with full access to their banking