THE Star ONLINE

M'sia sees biggest mobile data breach

NATION

Tuesday, 31 Oct 2017

By **Royce Tan** and **Sharmila Nair**

PETALING JAYA: The personal details of some 46.2 million mobile number subscribers in Malaysia are at stake in what is believed to be one of the largest data breaches ever seen in the country.

From home addresses and MyKad numbers to SIM card information, the private details of almost the entire population may have fallen into the wrong hands.

Malaysia's population is only around 32 million, but many have several mobile numbers. The list is also believed to include inactive numbers and temporary ones bought by visiting foreigners.

With this leak, Malaysians may be vulnerable to social engineering attacks and in a worst-case scenario, phones may be cloned.

It is also said that 81,309 records from the Malaysian Medical Council, Malaysian Medical Association (MMA) and Malaysian Dental Association were also leaked.

The leak of the mobile data was reported earlier this month on online forum and news site *lowyat.net*, which reported that it was thought to originate from a massive data breach in 2014.

Yesterday, the site "confirmed" that 46.2 million mobile numbers were leaked online.

Lowyat.net founder Vijandren Ramadass told *The Star* that all information it received on the matter was handed over to the Malaysian Communications and Multimedia Commission (MCMC).

Asked what sort of action would be needed, he said: "Telcos need to admit that this breach actually happened and should inform all their customers what should be done."

It is believed that the MCMC and police are collaborating on the investigation.

Network and security strategist Gavin Chow said the most common social engineering attack examples were phone and messaging scams.

"Scammers pretend to be someone calling or texting from the telco since they can prove they have the target's personal details," said Chow, who is with cybersecurity and malware protection company Fortinet.

He added that the scammers would then try to trick the victim in various ways.

These include transferring funds into their accounts and installing "telco applications" containing malware or spyware, which will be used to exploit the target in future.

"The devices would likely not be hacked directly, but anyone with the data dump information and a little creativity may convince unsuspecting victims to install malware on their devices.

"Users need to be alert when receiving calls and messages from strangers. Do not get tricked into sharing more personal details, transferring funds or installing apps," he said.

Technology strategist Dinesh Nair said there was not much that consumers could do, but they should change their SIM card, for starters.

"Your name, address, phone number, the IMSI (international mobile subscriber identity) and the IMEI (international Mobile Equipment Identity), which are tied to your device are all out there.

"I'm sure my data is there as well. People with really good technical skills will be able to clone someone's phone and that's the worst-case scenario," he said.

Dinesh added that while no one knew where the breach occurred, the fact that the details were out there pointed to a leak of some sort.

"How it happened, we can't tell but with so much released from different telcos at the same time, it must come from a single source," he added.

Bar Council cyber law and information technology committee co-chairman Foong Cheng Leong said assuming that the leak was after the enforcement of the Personal Data Protection Act 2010, there might have been a breach of the Act's Security Principle by the data users.

"The Security Principle requires data users to process personal data securely, but there is not much customers can do other than file a complaint with the Personal Data Protection Commissioner," he said.

Digi said in a statement that it prioritised the privacy of its customer data.

"The authorities are looking into the matter and we'll continue to support them," the statement read.

Celcom Axiata Bhd said it was "collaborating closely with the authorities to assist in the investigation", a sentiment echoed by Maxis Bhd, which also said it "fully supports the investigation".

Representatives from U Mobile declined to speak about the leak, while representatives of TuneTalk could not be contacted for comments at press time.

MMA president Dr Ravindran R. Naidu said a police report was lodged more than a week ago when news of the leak surfaced.

"Of course, no system is unhackable. Even the US Department of Defence has been hacked.

"However, we have been in the process of upgrading our IT system for the last year or so and the new servers will be more secure.

"We will also be upgrading our operational security measures and introducing a new SOP for our staff to minimise the risk of a repeat of this episode," he said.

Related story:

Data breaches nothing new, says expert

TAGS / KEYWORDS:

Courts Crime , Data Breach