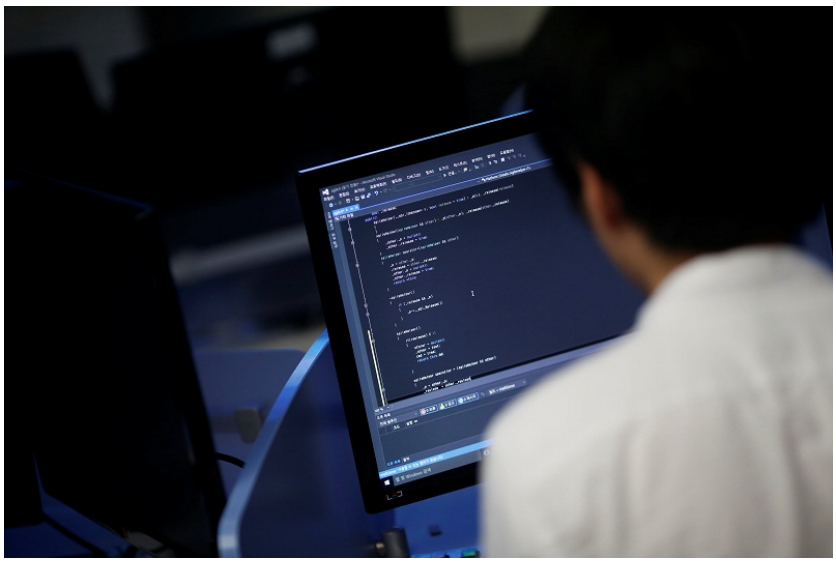
malaymail online

Malaysia

# We knew about data theft since February, dental group now says

BY AZRIL ANNUAR
NOVEMBER 01, 2017



Yesterday MCMC met with telecommunications companies over the alleged sale of consumer data believed to be obtained illegally. — Reuters pic

KUALA LUMPUR, Nov 1 — The Malaysian Dental Association (MDA) disclosed today that it had been alerted to a security breach on its online information system containing private data of its members since February.

Its president Dr Ng Woan Tyng said the association was first informed of the breach and theft on February 14 by CyberSecurity Malaysia and Malaysia Computer Emergency Response Team (MyCERT), which were hired to guard its digital networks.

The breach was first noticed by a foreign security organisation — which Dr Ng did not name — which then alerted CyberSecurity Malaysia that MDA's database content, including personally identifiable information such as email addresses and login credentials had been compromised, she explained.

"We were requested to assist in the investigation of the above matter and to reset passwords for the affected machines and users accordingly.

"In addition, we were requested to forward to the MyCERT any logs or malware/trojan files extracted from the machine in order for them to conduct further analysis," Dr Ng told Malay Mail Online when contacted for comment on the massive personal data leak affecting 46.2 million Malaysians, which the Communications and Multimedia Ministry is now investigating.

She said MyCERT informed the association that MDA's host server system appeared to have been hacked.

Since MDA had no control over the host server, it quickly switched over to a new server provider in March without waiting for any further evidence on the data breach. She added that MDA has also upgraded its firewall to protect against unauthorised access.

Dr Ng said the data leak as highlighted last month by tech news portal Lowyat.net now supports the alert from CyberSecurity Malaysia in February that MDA's system has been hacked into since January 21 five years ago.

"The Malaysian Communications and Multimedia Commission (MCMC) was alerted by our programmer concurrently, and we have been advised to lodge a police report, which has already been done at the time of publication," she said.

Dr Ng added that MDA has also advised its members to regularly reset personal passwords for the login account to "prevent further fraudulent activities".

MDA did not respond to *Malay Mail Online's* additional query as to why the incident was not immediately reported to the authorities in February.

The Malaysian Medical Association (MMA) told Malay Mail Online when contacted that it was unaware of the data theft until the matter was reported by Lowyat.net on October 19, but took immediate action to beef up its cybersecurity.

MMA president Dr Ravindran R. Naidu confirmed a police report has been made and they are working together with the authorities.

“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,” said Dr Ravindran.

MMA said their stolen data contains names, phone numbers and IC numbers of its members.

“It is unlikely that this will cause any serious problems, but the possibility exists that members may receive unsolicited SMS or email spam,” he said.

Lowyat.net first reported network security breaches in several Malaysian telecommunications companies as well as the persona data of several medical groups of some 46.2 million mobile phone numbers on its website October 19.

The technology news site said the leak included postpaid and prepaid numbers, customer addresses as well as sim card details from all major operators including DiGi, Celcom, Maxis, Tunetalk, Redtone and Altel.

Yesterday MCMC met with telecommunications companies over the alleged sale of consumer data believed to be obtained illegally.

Subsequently, the Communications and Multimedia Ministry said earlier today it has identified possible suspects behind the theft and attempted sale of the information.