Persatuan Pengguna Pulau Pinang
Consumers Association of Penang
槟城消费人协会 பினாங்கு பயனீட்டாளர் சங்கம்

Websites:
www.consumer.org.my

10 Jalan Masjid Negeri, 11600 Pulau Pinang, Malaysia
Tel: 604-8299511 Fax: 604-8298109
email: consumerofpenang@gmail.com

Letter to the Editor **24 February 2016**

RIGHT TO CONFIDENTIALITY OF PERSONAL HEALTH DATA VIOLATED

The Consumers' Association of Penang (CAP) is distressed by the recent news that a group of hackers have hacked into the systems of both government and private hospitals and stolen the personal health data of tens of thousands of individuals - data which is then sold to pharmaceutical companies through information selling syndicates.

The implications of this cyber theft is terrifying because our government and various agencies are trying to get everything (banking transactions, filling forms, making complaints, etc.) to go "online", as part of our green initiative; however, there is a high chance we don't really have the security to back this move – as made obvious by this incident. As it is, a news report has stated that 10,000 cyber crime cases are reported each year with an approximation of money loss equalling more than RM2.7 million; and the crimes largely involve online scams and hacking of computer servers.

This breach in privacy is no laughing matter and must be taken seriously. Many people may not realise this, but information related directly to them has been obtained against their will and is now being bartered between unscrupulous individuals for profit. Ultimately, drug companies are at the end of this chain - using this unlawfully obtained information to make more money out of the victims.

Also consider that we cannot be certain that pharmaceutical companies are the only ones buying this information? There may be companies in many other sectors that could benefit from possessing this information, for example insurance companies.

This incident should be a clear indication to us that if a group of hackers can overcome the security in both government and private hospitals so easily to steal personal health data, they can also steal some other set of personal data and sell it to the highest bidder ... for instance, banking information. This could already be happening and it just has not been detected yet.

Despite this, the agencies responsible for our cyber security have put onus on the public, be it businesses or individuals, to report if they notice their computer servers being tampered with so that they can stop any data theft. This is obviously not a sufficient way to handle the issue. By the time anyone realises there is something wrong with their computer servers it's probably already too late...unless the individual is a hacker themselves.

In light of this, CAP suggests that:-

- Agencies such as Cyber Forensics Intelligence Centre (CyberFIC), CyberSecurity Malaysia (CSM) and the Malaysian Communication and Multimedia Commission (MCMC), need to nip this problem in the bud by tracking and stopping the hackers who steal this information.

- The companies - such as the pharmaceutical companies in this case – that buy this information should be charged with having committed a criminal offense by possessing personal data illegally. If there is no market for unlawfully obtained personal data then stealing the information becomes redundant.

- MCMC, CyberFIC and CSM, as the responsible agencies, need to beef up our cyber security immediately.

S. M. Mohamed Idris
President
Consumers Association of Penang