THE BUSINESS TIMES

Published November 7, 2011

THIS WEEK'S TOPIC

Tackling cyber-fraud

From your experience, is cyber-fraud a genuine threat and are online users sufficiently aware of the dangers? What should consumers, companies and the authorities do to minimise the threat?

Toby Koh
Group Managing Director
Ademco Security Group

SECURITY is never convenient. And that is in conflict with common human instinct for simplicity. Cyber-fraud is well publicised in the media and yet, many consumers will ignore the dangers for the pleasure of convenience. In the course of our business in the security industry, we encourage our clients to consider a mandatory change of password for all users of the security system in a pre-determined time period. Hence, every three months, the security system will ask the user for a new password without any exceptions.

In addition, we advocate a two-factor authentication policy. Users must possess a smart card (physical token) as well as a password (intangible data) in order to be granted access. This is best practice. In the e-commerce space, a password is simply not good enough. Two-factor authentication should be the norm. The extent and sophistication of the authentication should be assessed against the potential risk to determine the investment in security that may be necessary.

Companies which display a noted concern for the security of their customers and staff will receive increased loyalty and public awareness.