OFTA talks anti-spam with ACMA

Representatives of the Office of the Telecommunications Authority (OFTA) in Hong Kong recently visited ACMA's Melbourne office to discuss ACMA's anti-spam strategies.

The Hong Kong Government is in the process of introducing anti-spam legislation. It has decided to adopt 'opt-out' legislation, similar to the United States 'Can-Spam' Act, instead of 'opt-in' legislation like the Australian Spam Act. In an opt-out regime, companies can send electronic messages to potential customers until the recipient chooses to unsubscribe. In Australia, a sender needs the consent of the recipient before a commercial electronic message can be sent.

Hong Kong intends to supplement its opt-out regime with separate 'do-not-contact' lists for voice telephony, fax and short message service. Businesses and consumers will therefore be able to opt out of all marketing via a certain medium by simply registering on the relevant list.

The proposed legislation also includes marketing via recorded voice telephone calls. In Hong Kong, local calls are free and as a result, many companies use recorded voice messages as a low-cost form of marketing. Fax marketing (currently excluded from Australia's Spam Act) will also be covered by the new law.

LEFT TO RIGHT: OFTA'S ASSISTANT DIRECTOR, SO TAT-FOON, ACMA'S SANDY KNOWLES, HEATHER NEATE AND JACKIE FAM, OFTA'S REGULATORY AFFAIRS MANAGER, ELVIN LAM, AND HEAD OF INFORMATION AND COMMUNICATIONS TECHNOLOGIES, HENRY CHANG

If an email seems **phishy**, don't take the bait

ACMA has renewed its warning to consumers to take precautions against 'phishing', as part of a four-week campaign by the Australasian Consumer Fraud Taskforce to help people protect themselves from scams.

'Phishing' refers to fraudulent messages usually sent via email (or in some cases a telephone call) and used to gain illicit access to personal and banking information. These messages appear to come from legitimate businesses, most commonly financial institutions. They are designed to lure recipients into disclosing personal data such as bank account numbers, passwords and credit card numbers, which are then used to commit fraud.

The Australian Bankers Association has advised that banks and other financial institutions will NEVER initiate a telephone call or email asking for your password, PIN or personal banking details.

Phishing isn't new. What is new is the increased intensity and technical sophistication of phishing scams. They come in different shapes and sizes, but they all share a common purpose—to trick people into disclosing personal details such as PINs and passwords or to click on a link that downloads a dangerous code that can capture personal information.

The ploys used appear legitimate, such as asking people to supply personal information in response to warnings about 'security and maintenance upgrades', 'investigation of irregularities' or 'bills or charges due.

More and more of these attacks are being committed by sophisticated crime gangs. The increasing sophistication of the scams means they can all too easily slip under the guard of many computer and internet users. Phishing scams often originate from overseas?once Australians respond and money or personal information has gone offshore, it is extremely difficult to recover or police.

ACMA advises that people should not respond to emails asking for confidential information, account details or passwords. Customers should only visit a bank, retailer or credit card website directly by typing a known website address themselves into their internet browser, or by using their Favourites list—not by clicking on email links.