

# AWASI web perbankan Internet palsu

Source : Utusan  
Malaysia

Date : 21 Dec 2009

Page : 20

KUALA LUMPUR 20 Dis. – Perbuatan mencuri maklumat menerusi Internet semakin meningkat, demikian menurut nasihat oleh Pusat Bantuan Cyber999 CyberSecurity Malaysia.

Pusat Bantuan Cyber999 menerima banyak laporan daripada pengguna Internet mengenai laman-laman web yang hosnya dari luar negara. Ia seperti beberapa laman web e-perbankan bank-bank terkemuka di negara ini.

Laman-laman web penipuan ini atau laman-laman web palsu digunakan untuk 'serangan mencuri' yang memanipulasi kelemahan keselamatan manusia. Ia dilakukan dengan mencero boh entiti sebenar, sebagai contoh, meniru laman web perbankan biasa.

'Serangan mencuri' ini juga menggunakan taktik kejuruteraan sosial seperti menghantar e-mel *spam*, katanya menerusi satu kenyataan di sini hari ini.

Kandungan e-mel terbabit menggunakan perkataan-perkataan yang meyakinkan untuk menipu orang ramai supaya membuka hubungan yang akan membuka laman-laman web perbankan palsu.

Memandangkan laman-laman web itu sama seperti laman web sebenar, pelanggan terpedaya dengan memasukkan maklumat sulit, seperti nama pengguna dan kata laluan e-perbankan ke dalam laman web e-perbankan palsu itu.

Menerusi cara itu 'serangan mencuri' mudah mencuri nama pengguna dan kata laluan pelanggan bank yang tidak mengesyakinya.

Bank-bank tidak pernah meminta pengguna membuat kemas kini, menukar semula kata laluan, membuka akaun atau apa sahaja berkaitan perbankan menerusi e-mel dan URL.

"Jika anda menerima e-mel sama seperti daripada bank atau institusi perbankan, nasihat kami ialah abaikannya.

"Jika anda curiga, sila hubungi bank anda untuk tujuan pengesahan atau hubungi Pusat Bantuan Cyber999, kata Ketua Pegawai Eksekutif CyberSecurity Malaysia, Lt. Kol (B) Husin Jazri.

**KUALA LUMPUR:** The number of phishing attempts is on the rise, according to an advisory released by the Cyber999 Help Centre of CyberSecurity Malaysia.

The Cyber999 Help Centre has been receiving numerous reports from Malaysian Internet users regarding phishing websites hosted overseas.

These look exactly like that of Malaysian banks' e-banking websites.

These phishing websites or fake websites are used to conduct a "phishing attack", which involves manipulating the weak side of human security.

This is done by masquerading as a trustworthy entity, for example, a copycat of a familiar banking website.

The "phishing attack" also uses a kind of social engineering tactic, such as sending spam emails that look as though they have been sent by a well-known Malaysian bank, it said here

yesterday.

The email tricks people into clicking on a link that will open up the phishing website or fake e-banking website.

As the fake website looks exactly like the original, customers enter confidential information such as e-banking usernames and passwords into the fake e-banking website.

This way, the "phishing attacker" steals usernames and passwords of bank customers.

CyberSecurity Malaysia chief executive officer Lt-Col (Rtd) Husin Jazri said: "If you do receive such emails and they look like they are from banks or financial institutions, our advice is to ignore them.

"If you do get suspicious, contact your bank for verification or contact our Cyber999 Help Centre."

CyberSecurity Malaysia is under the purview of the Science, Technology and Innovation Ministry. — Bernama