Diskusi ICT

Bersama **FIRKHAN**
sembangict@yahoo.com

Waspada serangan *pishing*

APAKAH itu serangan *phising* dalam dunia siber?

- SULAIMAN AKHLAKEN, KL.

Apabila dibunyikan perkataan *phising* ini ia berbunyi *fishing* iaitu memancing dan konsep memancing ini juga wujud dalam aktiviti *phising*.

Aktiviti *phising* ini bukan memancing ikan tetapi ia memancing maklumat penting dalam dunia siber dengan tujuan tertentu seperti nombor akaun bank, nombor kad pengenalan, kata laluan sesebuah akaun web dan lain-lain.

Jadi, *phising* adalah proses mengumpan seseorang untuk mendapatkan maklumat peribadinya menerusi teknik komunikasi elektronik seperti e-mel, talian telefon, laman web dan lain-lain.

Seterusnya, dengan maklumat tadi si pelaku akan melakukan penyamaran seperti pemilik maklumat sebenar.

Penyamaran ini dikenali sebagai *Identity Theft* atau pencuri identiti seseorang.

Ciri-ciri serangan *phising*

1. Permintaan menerusi e-mel untuk dapatkan maklumat peribadi atau pengemaskinian maklumat peribadi seperti nombor kad kredit dan sebagainya.
2. Terdapat ciri-ciri keperluan yang mendesak atau diperlukan segera seperti akaun bank tidak akan aktif sekiranya pengemaskinian maklumat tidak dibuat.
3. Penggunaan panggilan secara umum seperti pelanggan dan tidak menggunakan nama sebenar pengguna atau pelanggan.
4. Kadang-kala bersama dengan e-mel terdapat sisipan fail yang berkemungkinan besar adalah malware.
5. Terdapat sambungan ke laman web palsu. Alamat URL laman web palsu ini juga kadang-kala menggunakan alamat singkat atau seakan-akan laman web asli seperti *http://www.uthmim.edu.my*. Laman web yang dipaparkan juga seolah-olah hampir sama dengan yang asli.
6. Terdapat kesilapan tatabahasa atau ejaan dalam ayat yang digunakan.
7. Kebiasaan laman web yang melibatkan transaksi seperti pihak bank dan sebagainya mengunakan protokol HTTPS berbanding protokol HTTP. Jadi, di awal laman webnya akan bermula seperti *https://www.uthm.edu.my*.

Langkah-langkah Pencegahan

1. Sekiranya menerima e-mel yang disangsi, jangan sesekali mengklik alamat URL yang ada di dalamnya atau memuat turun fail sisipan yang ada.
2. Jangan sesekali membalas e-mel yang disangsi itu dengan maklumat peribadi.
3. Penggunaan pelayar web yang mempunyai fungsi perlindungan daripada serangan Phising laman web.
4. Lakukan pengemaskinian bagi perisian anti-virus yang digunakan.
5. Aktifkan penggunaan fungsi tapisan e-mel sampah pada akaun e-mel yang digunakan.