Tutorial ICT

Bersama FIRKHAN
sembangict@yahoo.com

Kaedah kesan serangan *phising*

TAKTIK serangan dan penipuan di alam siber dikenali sebagai *phising* menjadi masalah seawal wujudnya dunia Internet sehingga sekarang.

Serangan *phising* boleh menyebabkan berlakunya kehilangan wang dalam perbankan Internet, penyebaran *malware*, pemula serangan *ransomware*, kecurian data peribadi dan sebagainya di alam maya. Dilaporkan bahawa syarikat Facebook dan Google menjadi mangsa serangan ini pada tahun 2017.

Sudah semestinya pasti ada cara untuk mencegah serangan pancingan data atau *phising* ini bagi membolehkan pengguna internet melihat dan memadam mesej berbahaya seperti itu menerusi e-mel dan aplikasi media sosial.

Dibincangkan beberapa kaedah untuk mengesan serangan *phising* ini pada peringkat awal.

1 Penggunaan perisian antivirus yang sentiasa dikemas kini keselamatannya.

2 Keselamatan gerbang masuk menerusi e-mel dan capaian laman sesawang (*web*) dipertingkat keselamatannya terutama keupayaan perisian keselamatan yang digunakan untuk menapis kandungan mesej yang

3 Tingkatkan kesedaran keselamatan siber dalam kalangan para pengguna dengan pelbagai cara termasuk latihan dan ujian simulasi serangan.

4 Pemahaman pelbagai jenis penipuan pancingan data akan menyediakan persediaan terbaik bagi pengguna bagi serangan *phising* yang paling disasarkan.

5 Aplikasi e-mel perlu menggunakan penapisan kandungan dan tanda tangan yang membolehkan pengelakan berlaku terhadap banyak e-mel berniat jahat dibuka.

6 Sekiranya perlu, aplikasi e-mel boleh diperlengkap dengan fungsi yang lebih canggih dalam mencegah serangan *phising* iaitu fungsi analisis kelakuan pengguna dan profil peti mel.

7 Penguatkuasaan pengesahan pelbagai faktor ke atas pengguna terutama bagi yang mengendalikan maklumat paling sensitif.

8 Fungsi pencegahan serangan dengan gabungan analisis tingkah laku, profil peti mel, automasi forensik dan maklum balas boleh mewujudkan pendekatan pencegahan pelbagai lapisan yang holistik. Menggunakan maklumat perisikan dan kecerdikan pengesahan e-mel yang dipancing ini dapat membantu organisasi secara proaktif mempertahan gerbang rangkaian dan kandungannya.

9 Galakkan pembuatan laporan oleh pengguna terhadap mana-mana mesej atau e-mel jelik dan dicurigai.