Publication: Berita Harian
Date: 1 Feb 2022
Headline: Phishing cases are an 'eye opener' to cyber threats

Kes pancing data 'buka mata' tentang ancaman siber

Lebih banyak usaha boleh dijalankan untuk tingkat perlindungan

▶ERVINA MOHD JAMIL
ervinamj@sph.com.sg

KES penipuan pancingan data (phishing) menerusi khidmat pesanan ringkas (SMS) – yang dikenali sebagai *smishing* – terhadap pengguna bank baru-baru ini adalah satu peringatan bahawa penjenayah siber akan terus cuba melemahkan sistem bank dan, oleh itu, bank dan pengguna harus sentiasa berjaga-jaga.

Sementara pelbagai usaha dijalankan untuk memperkukuh perlindungan, penjenayah siber juga akan sentiasa berusaha mengatasi benteng pertahanan ini.

Berkata demikian ketika dihubungi *Berita Harian* baru-baru ini, beberapa ahli akademik dalam bidang keselamatan siber berkata, ini juga bermakna strategi keselamatan siber Singapura harus terus berkembang bukan sahaja untuk mengenal pasti apa yang boleh dilakukan penjenayah siber sekarang, tetapi juga cuba mengenal pasti apa yang mereka mungkin lakukan pada masa akan datang serta membina perlindungan terhadap ancaman itu.

Penolong Profesor Goh Weihan, yang mengajar program ijazah Keselamatan Maklumat di Institut Teknologi Singapura (SIT), berkata kejadian *smishing* baru-baru ini menunjukkan beberapa kegagalan dalam rantaian keselamatan siber dan apabila kesemuanya berlaku pada masa yang sama, ini membolehkan penjenayah siber di sebalik kejadian itu berjaya meraih matlamatnya.

"Ini termasuk pelaku yang boleh memalsukan ID penghantar SMS bank untuk menghantar SMS yang kononnya daripada bank, pelanggan yang klik pautan dalam SMS tanpa memeriksa sama ada pautan itu sah serta bank yang membenarkan beberapa tindakan berisiko tinggi diambil tanpa halangan dan kemudian... kurang memberi sokongan sejurus selepas penipuan terjadi.

"Kalau salah satu daripadanya tidak berlaku, penipuan itu mungkin tidak akan terjadi," kata Dr Goh.

Pengurus Kanan Sekolah Teknologi Infokom di Politeknik Ngee Ann (NP), Encik Mohd Saifulamri Omar, berkata penghubung paling lemah dalam keselamatan siber biasanya adalah manusia.

"Adalah lebih sukar bagi penjenayah siber melemahkan *server*, rangkaian dan proses pertubuhan kerana langkah kawalannya dipertahan dan dipantau dengan rapat.

"Namun, ini berbeza bagi pengguna. Kita boleh mudah... ditipu untuk mendedahkan butiran akaun atau peribadi apabila pelaku mengambil kesempatan ke atas emosi kita seperti rasa takut, tamak dan sebagainya," ujar beliau.

Sementara serangan pancingan data boleh dikurangkan, Profesor Madya Chang Ee-Chien daripada Sekolah Komputing Universiti Nasional Singapura (NUS) berkata ia tidak dapat dihapuskan.

"Namun ini tidak bermakna kita hanya berdiam diri tanpa mengambil langkah perlindungan.

"Dari segi teknikal, sistem dan aliran kerja boleh dirancang untuk mengurangkan kesilapan pengguna.

"Aspek lain seperti meningkatkan kesedaran orang awam tentang kebersihan siber dan pengurusan kejadian yang berkesan juga boleh membantu," ujar Dr Chang.

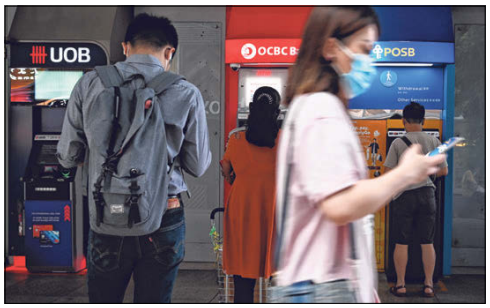
Malah tambahnya, langkah yang diumumkan Penguasa Kewangan Singapura (MAS) dan Persatuan Bank Singapura (ABS) baru-baru ini untuk menghapuskan sebarang pautan yang boleh diklik dalam SMS atau e-mel kepada pelanggan merupakan satu langkah yang amat baik.

Sedang kejadian baru-baru ini telah mewujudkan lebih kesedaran tentang hal ini, dengan lebih banyak perbincangan serius diadakan berhubung-nya, lebih banyak usaha boleh dijalankan untuk meningkatkan perlindungan terhadap penipuan sedemikian.

Dengan landskap ancaman yang terus tidak menentu, Encik Mohd Saifulamri berkata adalah wajar usaha dijalankan untuk belajar daripada episod ini dan kemudian mengukuhkan langkah kawalan keselamatan.

Menurut Dr Goh, bagaimana Singapura melatih pengamal keselamatan siber pada masa akan datang juga harus dipertimbang.

"Di SIT, kami melatih bakat keselamatan siber untuk mempertahan daripada (ancaman yang wujud) sekarang dan melatih mereka bersifat tangkas serta memahami pemikiran penyerang untuk memikirkan bagaimana penyerang boleh mengeksploitasi sistem dan menilai bagaimana untuk melindunginya," kata beliau.



KESELAMATAN SIBER DIGUGAT: Kes penipuan pancingan data menerusi SMS melibatkan pengguna bank adalah satu peringatan untuk sentiasa berjaga-jaga. Gambar menunjukkan orang awam menggunakan mesin ATM beberapa bank di luar Bishan MRT bulan lalu. – Foto fail

> "...Ini termasuk pelaku yang boleh memalsukan ID penghantar SMS bank untuk menghantar SMS yang kononnya daripada bank, pelanggan yang klik pautan dalam SMS tanpa memeriksa sama ada pautan itu sah serta bank yang membenarkan beberapa tindakan berisiko tinggi diambil tanpa halangan dan kemudian... kurang memberi sokongan sejurus selepas penipuan terjadi. Kalau salah satu daripadanya tidak berlaku, penipuan itu mungkin tidak akan terjadi."
>
> **– Penolong Profesor Goh Weihan, Institut Teknologi Singapura (SIT).**

TIP LINDUNGI DIRI DARIPADA MENJADI MANGSA PANCINGAN DATA

- **Jangan klik pautan dalam mesej SMS yang kelihatan dihantar oleh bank; taip laman web bank di pelayar web (browser) atau gunakan aplikasi bank**
- **Jika ragu-ragu, hubungi bank untuk mengesahkan maklumat yang diterima menerusi SMS**
- **Jangan beri butiran bank anda kepada sesiapa**
- **Gunakan alat sendiri untuk menjalankan sebarang urus niaga**
- **Pastikan alat anda sentiasa dikemas kini dan sering pantau akaun anda**
- **Pastikan terdapat simbol mangga di tempat anda taip laman web dan nama domain sama dengan nama pertubuhan; sebarang bentuk variasi mungkin menunjukkan laman web itu palsu**

Sumber: Profesor Madya Chang Ee-Chien daripada Sekolah Komputing Universiti Nasional Singapura (NUS), Penolong Profesor Goh Weihan yang mengajar program ijazah Keselamatan Maklumat di Institut Teknologi Singapura (SIT)