PERSATUAN BANK BANK DALAM MALAYSIA
THE ASSOCIATION OF BANKS IN MALAYSIA

Headline: Kenali taktik licik si penipu siber
Publication/Portal: Kosmo
Date: 22 January 2019

Language: Malay
Section: Kosmo2
Page: 24

PENJENAYAH siber kini semakin licik dengan pelbagai taktik digunakan bagi memperdaya mangsa.

ORANG ramai perlu peka dan berhati-hati sebelum melakukan apa-apa akses melibatkan maklumat peribadi.

Kenali taktik licik si penipu siber

AGENSI pakar sekuriti dan teknikal siber kebangsaan, Cybersecurity Malaysia melaporkan bahawa sebanyak 60 peratus daripada 1,302 kes di negara ini yang diterima antara Januari hingga April 2018 merupakan aduan yang melibatkan penipuan siber.

Hal ini mendapat perhatian perbadanan multinasional dari Amerika Syarikat, Fortinet yang mahu pengguna internet di Malaysia supaya mengelakkan diri daripada menjadi mangsa penipuan siber.

Pakar Strategis Keselamatan dan Rangkaian Fortinet, Gavin Chow berkata, penjenayah siber kini semakin licik dan mereka menggunakan pelbagai taktik penipuan untuk mendapatkan akses kepada peranti atau rangkaian, memeras wang serta mencuri maklumat yang berharga.

GAVIN

"Oleh kerana pengguna terus menyambung lebih banyak peranti ke rangkaian, risiko penipuan boleh berlaku menyebabkan ia semakin meningkat.

"Orang ramai perlu peka dan berhati-hati sebelum melakukan apa-apa akses yang melibatkan maklumat peribadi dan rangkaian. Ini bertujuan bagi melindungi maklumat tidak disalah guna oleh penjenayah siber semasa rangkaian disambungkan," ujarnya menerusi satu kenyataan baru-baru ini.

Beliau menambah, orang ramai perlu memahami jenis-jenis penipuan siber bagi melindungi maklumat berharga sekali gus mengelakkan diri daripada menjadi mangsa jenayah siber.

Dalam usaha memberi kesedaran berhubung jenayah siber, Fortinet menyenaraikan enam penipuan siber umum yang sering digunakan untuk menyasarkan pengguna di Malaysia.

1. Penipuan *phishing*

Serangan *phishing* berlaku apabila seorang penjenayah menghantar komunikasi seperti e-mel, panggilan telefon dan teks, berpura-pura menjadi orang lain untuk mengekstrak atau mengakses kelayakan, data peribadi, maklumat kewangan atau maklumat sensitif. Dianggarkan 59 peratus daripada semua *ransomware* yang berjaya dijangkiti adalah diangkut melalui penipuan *phishing*. Untuk lebih mengenali penipuan berniat jahat ini, periksa nama penghantar apabila anda menerima komunikasi daripada sumber yang anda tidak kenali.

2. Penipuan *spear-phishing*

Penipuan *spear-phishing* adalah melakukan penyelidikan mendalam tentang mangsa dan mereka meluangkan masa untuk memahami mangsanya bagi meningkatkan peluang kejayaan.

3. Penipuan *baiting*

Penipuan *baiting* bertujuan mengumpan pengguna yang tidak curiga untuk melakukan tindakan tertentu seperti memuat turun virus atau memasukkan maklumat peribadi sebagai pertukaran untuk 'umpan'. Jenis penipuan ini mempunyai banyak bentuk dan matlamat akhirnya adalah memikat pengguna untuk memasang sesuatu dengan berniat jahat.

4. Penipuan sokongan teknikal

Penipu akan bertindak sebagai pekerja sokongan teknologi, sama ada bekerja untuk organisasi mangsa atau untuk perkhidmatan bebas, bagi mendapatkan akses kepada maklumat peribadi.

5. Mengamankan peranti mudah alih

Aplikasi palsu yang digunakan untuk perlombongan data atau *ransomware* adalah tersedia secara meluas, terutama untuk sistem operasi Android.

6. Peranti *internet of things* (IoT)

Banyak peranti IoT yang mudah dieksploitasi mempunyai sambungan Internet yang berterusan dan menggunakan *graphics processing unit* yang kuat, menjadikannya sempurna untuk perlombongan kripto dan eksploitasi *distributed denial of service* (DDoS).