Waspada taktik scammer elak jadi mangsa

Oleh Dr Normalia Samian
bhrencana@bh.com.my

Pensyarah Kanan, Jabatan Teknologi Komunikasi dan Rangkaian Fakulti Sains Komputer dan Teknologi Maklumat, Universiti Putra Malaysia (UPM)

Sehingga kini, isu keselamatan siber tetap menjadi antara perhatian utama di Malaysia. Kes seperti pencerobohan keselamatan data peribadi, pancingan data, buli siber dan pelbagai jenis penipuan dalam talian dilihat semakin meningkat.

Walaupun diberi peringatan di pelbagai sumber media seperti iklan di televisyen dan radio, kempen kesedaran di laman sosial dan sebagainya, kes ancaman keselamatan siber tetap berlaku serta menunjukkan trend membimbangkan.

Polis Diraja Malaysia (PDRM) sebelum ini mendedahkan lebih RM155 juta nilai kerugian direkodkan melalui 3,604 kes penipuan siber sepanjang tempoh lima bulan pertama tahun ini.

Terbaru, Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM) mendapati berlaku insiden penyamaran dan penipuan melalui kaedah pengambilalihan akaun aplikasi sembang (*chat*) seperti SMS, sistem sembang Facebook, Instagram, WhatsApp dan sistem emel semakin meningkat.

Sebagai rekod, statistik trend aduan awam diterima SKMM menunjukkan jumlah aduan berkaitan penggodaman dan kehilangan akses meningkat sebanyak 55 peratus, iaitu 1,599 aduan pada 2020 dan 2,483 aduan pada 2021.

Modus operandi penggodam adalah dengan melakukan penyamaran. Penipu yang berjaya menyamar sebagai ahli keluarga atau sahabat atau pihak berkuasa untuk memperdaya mangsa.

Persoalan pertama yang mungkin bermain di fikiran pengguna adalah bagaimana penyamaran boleh berlaku. Mengambil contoh aplikasi SMS, pelaku hasad (*malicious*) boleh memanipulasi lapangan identiti pengirim menggunakan alat Antara Muka Pengaturcaraan Aplikasi (API) untuk mengaburi nombor telefon sebenar mereka.

Guna gaya bahasa pelik

Terdapat pelbagai teknik berbeza membolehkan insiden pengambilalihan akaun sembang ini terjadi. Terdapat beberapa tip boleh dijadikan pedoman untuk mengenal pasti penipuan dan mengelakkan diri daripada menjadi mangsa.

Berdasarkan kes yang berlaku, penipu siber biasanya 'tergesa-gesa' kerana mereka ingin segera mendapatkan apa dihajati sebelum penipuan mereka terbongkar. Jika pengguna mendapati 'kenalan' berkelakuan pelik, segera hubungi kenalan anda melalui panggilan telefon untuk mendapatkan kepastian.

Penyamar biasanya menggunakan gaya bahasa pelik, justeru pengguna perlu memeriksa gaya bahasa dan lenggok komunikasi 'kenalan' yang berkomunikasi. Penyamar biasanya tidak akan dapat meniru bulat-bulat cara komunikasi orang lain.

Jika pengguna mengesyaki berlaku sesuatu mencurigakan dalam komunikasi bersama, ajukan beberapa pertanyaan menguji untuk menilai kesahihan 'kenalan' yang sedang berhubung.

Pengguna juga patut mengaktifkan 'dua langkah pengesahan' pada semua akaun media sosial dan aplikasi sembang. Apabila mekanisme keselamatan ini diaktifkan, aplikasi akan meminta pengguna menginput kod 4 hingga 6 digit ditetapkan berserta dengan kod pengesahan baharu. Dengan ini, rampasan akaun oleh pelaku hasad akan lebih sukar.

Pengguna dinasihatkan tidak sewenang-wenangnya klik sebarang pautan mencurigakan terutama jika pautan itu tidak menggunakan protokol 'https', kerana boleh mendedahkan pengguna kepada pemancingan data (*phishing*). Sekiranya pengguna menyedari sudah menjadi mangsa penipuan, hubungi bank dengan kadar segera.

Secara keseluruhan, tidak ada formula atau jaminan khusus boleh melindungi keselamatan diri dan data peribadi kita daripada terdedah kepada risiko penipuan siber.

Namun, jika pengguna sentiasa beringat dan mengambil langkah berjaga-jaga seperti disarankan, pasti boleh mengurangkan risiko ancaman pencerobohan data peribadi.

Pengguna perlu menanam sikap 'fikir berkali-kali' sebelum berkongsi sebarang maklumat data peribadi dengan sesiapa sahaja termasuk pasangan, ahli keluarga, adik beradik, saudara mara, kenalan dan sesiapa saja untuk mengelak menjadi mangsa penipuan *scammer*.