myMetro
PASAI BERITA SEBENAR

Tingkat pengetahuan teknologi

Muhammad Saufi Hassan
Disember 6, 2022 @ 7:00am

Pengguna memainkan peranan paling penting dalam mendepani insiden pencerobohan data peribadi dan ia tidak hanya terletak kepada tanggungjawab pihak berkuasa saja.

Jika pengguna tidak peka dengan keadaan semasa dan gemar menekan pautan meragukan serta memuat turun fail atau aplikasi yang berada di luar gedung maya, ia menambahkan kemungkinan bahawa data pengguna berada dalam keadaan bahaya.

Untuk itu, kunci kepada keselamatan data peribadi adalah kepekaan pengguna iaitu pemilik data berkenaan dan sentiasa berhati-hati ketika berada di ruang siber.

Kepekaan pengguna dapat menentukan sama ada data peribadi berada pada tahap selamat atau sebaliknya kerana pengguna adalah pemegang taruh utama dalam menjanjikan keselamatan data mereka daripada diceroboh, dimanipulasi serta digunakan oleh pihak ketiga.

CyberSecurity Malaysia (CSM) menerusi Pasukan Tindakbalas Kecemasan Komputer Malaysia (MyCERT) mencadangkan orang awam untuk melaksanakan amalan terbaik ketika berada di ruang siber.

CSM dalam satu peringatan menyatakan bahawa maklumat sensitif seperti nama, nombor telefon, emel dan alamat rumah yang terdedah mungkin didagangkan di laman web gela

p atau 'dark web' oleh penjenayah siber.

"Untuk itu, kita mencadangkan supaya pengguna hendaklah sentiasa berhati-hati terhadap individu atau organisasi yang meminta maklumat peribadi.

"Kebanyakan syarikat tidak akan meminta data sensitif daripada pelanggan mereka, jika diragui, pengguna harus mengesahkan dengan syarikat itu sendiri untuk mengelakkan sebarang isu yang berpotensi.

"Pengguna juga hendaklah sentiasa melihat dengan teliti nama paparan pengirim apabila menyemak kesahihan emel kerana kebanyakan syarikat menggunakan satu domain untuk URL dan emel mereka, jadi mesej yang berasal daripada domain yang berbeza ialah 'red flag'.

"Sebagai peraturan umum, pengguna tidak boleh menekan pautan atau memuat turun fail walaupun ia datang daripada sumber yang kelihatan 'boleh dipercayai' untuk mengurangkan risiko menjadi mangsa jenayah siber," katanya.

Orang awam yang mahu mendapatkan maklumat lanjut boleh melayari laman web MyCERT menerusi pautan https://www.mycert.org.my untuk advisori terbaru.

"Ketirisan data ini mungkin mengakibatkan serangan berbentuk pancingan data peribadi atau 'phishing' termasuk taktik serangan seperti 'smishing' atau 'vishing'.

"Kedua-dua bentuk serangan itu adalah penipuan di mana penjenayah cuba mendorong pengguna untuk menekan pautan penipuan melalui telefon, mesej teks, emel atau mel suara.

"Mangsa serangan pancingan data biasanya terpedaya dan ditipu untuk menekan pautan dan memasukkan maklumat sulit serta data sensitif seperti 'One Time Password' (OTP) atau kod keselamatan, butiran log masuk, kata laluan dan banyak lagi," katanya dalam satu advisori peringatan yang dikeluarkan susulan insiden kebocoran data.

Agensi itu turut menyatakan bahawa sebaik sahaja pelaku mendapat maklumat ini, mereka akan menggunakan maklumat terbabit untuk merampas akaun mangsa bagi tujuan kewangan.

Menurutnya, ini boleh dilakukan dengan menyamar sebagai mangsa atau menyalahgunakan akaun yang dicuri untuk aktiviti berniat jahat yang lain.