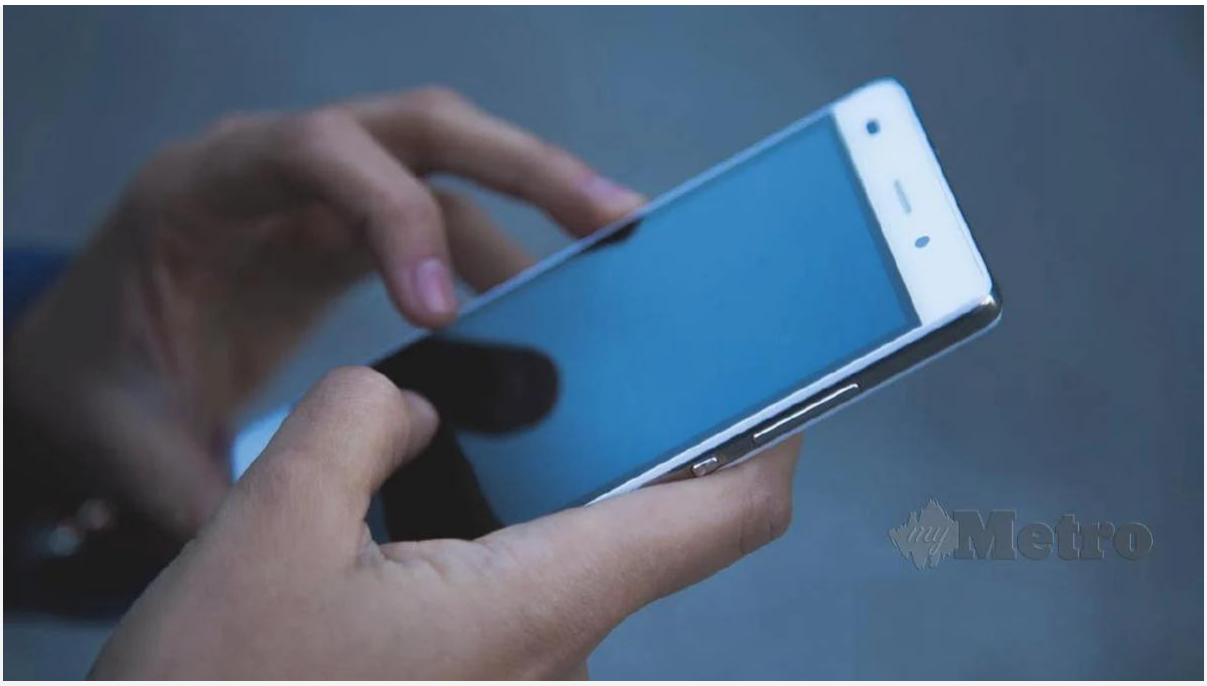
Jangan buat transaksi kewangan guna WiFi awam

BERNAMA



GAMBAR hiasan

Kuala Lumpur: Pengguna dalam talian yang menggunakan e-dompet dan kaedah e-pembayaran lain dinasihatkan supaya tidak menjalankan sebarang transaksi melalui sambungan WiFi awam.

Ketua Pembangunan Kriptografi CyberSecurity Malaysia, Hazlin Abdul Rani berkata, ancaman dan serangan daripada penggodam berlaku menerusi WiFi awam yang tidak selamat menyebabkan data peribadi dan mungkin semua maklumat akaun serta kelayakan log masuk boleh diakses semasa proses transaksi.

Beliau turut menasihatkan untuk lebih berwaspada mengenai kemungkinan penyerang menyamar sebagai rangkaian WiFi awam yang sah.

"Sebagai contoh, jika anda berada di lapangan terbang, nama WiFi adalah 'Lapangan Terbang ABC', namun penyerang itu mencipta WiFi dengan nama 'Lapangan Terbang ABC1', atau menukar huruf besar kepada huruf kecil WiFi untuk membuat anda percaya yang anda menggunakan WiFi yang sah. Kekeliruan ini juga boleh mengheret pengguna terjerumus ke dalam perangkap mereka.

"Oleh itu, berhati-hati dan elakkan menggunakan WiFi awam. Sebaliknya, gunakan sambungan rangkaian selamat yang mempunyai kata laluan," katanya dalam

perbincangan panel maya yang dianjurkan oleh Yayasan Forum Ekonomi Islam Sedunia (WIEF), bertajuk "#iEMPOWER: e-Dompet - Menerima Transformasi Tanpa Tunai", hari ini.

Mengulas lanjut, Hazlin berkata, pengguna juga mesti berhati-hati dengan serangan kejuruteraan sosial yang menyasarkan mereka melalui panggilan telefon, mesej pada peranti mudah alih dan e-mel dengan perisian berniat jahat yang dilampirkan (perisian hasad).

"Disebabkan kekurangan maklumat, kita mungkin tidak menyedari serangan itu, terutamanya apabila anda menerima panggilan telefon dan menjawab soalan mengenai maklumat peribadi tanpa mengetahui orang ini adalah penipu yang berpura-pura menjadi pihak berkuasa, wakil bank atau polis, antara lainnya," katanya.

Daripada perspektif peniaga, beliau berkata, sistem dan sistem Butiran Jualan (POS) yang memerlukan pengimbasan kod QR mesti disulitkan untuk mendapatkan sebarang kebenaran yang diberikan.

Ini adalah untuk memastikan transaksi, data dan maklumat dalam sistem adalah selamat dan tidak ada orang lain yang mempunyai akses kepada data dan maklumat itu.

Beliau berkata, pembangun aplikasi seharusnya dapat memberikan perlindungan kepada pelanggan mereka yang akan menggunakan dan mendapat manfaat daripada teknologi mereka dalam era digital dan e-dagang ini.

Antara ciri keselamatan ialah memasukkan pengesahan faktor dua hala, yang memerlukan pengguna memberikan pengenalan biometrik dan Nombor Maklumat Peribadi (PIN) atau kata laluan.

Disiarkan pada: Jun 15, 2022 @ 4:56pm