Cara selamat kendali peranti mudah alih

BAGAIMANAKAH cara selamat untuk mengendalikan penggunaan peranti mudah alih seperti komputer tablet, telefon pintar dan lain-lain?

Idrus, Simpang Renggang.

Diskusi ICT

Bersama **FIRKHAN**
sembangict@yahoo.com

Terima kasih. Peralatan komputer mudah alih ini seperti komputer riba, komputer tablet dan telefon pintar bersifat mudah untuk dibawa yang mengundang perlbagai isu keselamatan seperti kehilangan dan kecurian. Isu-isu keselamatan bagi peralatan komputeran mudah alih bersifat fizikal ini telah dibincangkan dalam ruangan ini sebelum ini.

Selain itu, sifat mudah dibawa ke mana-mana sahaja pada peralatan komputeran mudah alih ini juga terdedah kepada persekitaran digital yang tidak selamat.

Di samping itu, peralatan komputeran mudah alih banyak digunakan untuk pelbagai tujuan tertentu seperti perkongsian fail, tempahan, pembayaran dan penghantaran laporan.

Oleh itu, penggunaan peranti mudah alih ini dengan selamat dan betul sangat diperlukan bagi mengelakkan berlakunya masalah yang tidak diundang.

Seterusnya dibincangkan beberapa perkara keselamatan yang boleh dipraktikkan dalam penggunaan peralatan komputeran mudah alih ini.

1 Penggunaan kata laluan yang kuat dan kental. Sekiranya perlu, gabungkan penggunaan kata laluan ini dengan teknik pengesahan biometrik. Sekiranya peranti tersebut dibekalkan dengan fungsi pengesahan dua faktor, gunakanlah fungsi pengesahan tersebut. Kata laluan yang digunakan perlu kompleks, panjang, pelbagai jenis aksara, sukar untuk diteka dan kerap ditukarkan.

2 Elakkan penggunaan perkhidmatan sambungan Wi-Fi percuma digunakan secara umum untuk orang awam. Sekiranya perlu menggunakan perkhidmatan sambungan Wi-Fi percuma, pastikan ia dilindungi dan selamat digunakan. Pastikan perkhidmatan Wi-Fi yang digunakan dienkrip sambungannya. Teknik enkrip WPA (Wi-Fi *Protected Access*) lebih selamat digunakan berbanding teknik enkrip WEP (*Wired Equivalent Privacy*). Pastikan apa-apa jenis sambungan tanpa wayar yang ada pada peranti mudah alih seperti Wi-Fi, Bluetooth dan sebagainya ditutup sekiranya tidak digunakan.

3 Penggunaan perkhidmatan atau aplikasi VPN (*Virtual Private Network*) untuk capai sambungan rangkaian dan Internet secara selamat. Penggunaan aplikasi VPN ini dapat melindungi pengguna daripada pelayaran web yang tidak selamat terutama laman web yang tidak menggunakan protokol keselamatan HTTPS (*Secure HTTP*).

4 Enkrip peranti mudah alih yang digunakan terutama untuk melindungi data di dalamnya.

5 Pemasangan apliksai anti-*Malware* sekiranya perlu.

6 Sentiasa mengemas kini perisian terutama sistem pengoperasian, perisian keselamatan dan mana-mana perisian yang kerap digunakan.

7 Elakkan pengguna fungsi *autofill* yang terdapat dalam aplikasi terutama ketika pelayaran laman web.

8 Pastikan log keluar setelah selesai penggunaan sesuatu aplikasi.

9 Pastikan memuat turun aplikasi daripada sumber atau stor yang dipercayai.