

Guna tablet Android dengan selamat

BAGAIMANAKAH cara untuk menggunakan sistem komputer tablet berasaskan Android secara selamat?

- Ahmad, KL.

Secara umumnya, mana-mana sistem komputer yang digunakan perlu ada kawalan dan pemantauan keselamatan sekiranya disambungkan kepada rangkaian komputer atau internet. Perkara ini perlu terutama untuk menghindarkan sistem komputer itu daripada dijangkiti atau dikompromi oleh mana-mana perisian tidak sepatutnya seperti Malware, virus dan lain-lain. Selain daripada itu, perkara ini dapat mengelakkan sistem komputer daripada dicerobohi oleh seseorang yang tidak bertanggung jawab seperti penggodam, pesaing dan lain-lain.

Sistem komputer berasaskan Android banyak digunakan dalam sesebuah komputer mudah alih seperti komputer tablet dan telefon pintar. Jadi, sifatnya yang mudah alih menyebabkan ia mudah hilang atau tercicir secara fizikal. Seterusnya dibincangkan beberapa cara khusus yang selamat boleh digunakan dalam mengendalikan sistem komputer berasaskan Android ini.

- 1** Kemas kini sistem Android dan aplikasi yang terdapat dalamnya dengan kemas kini yang terkini dan pasang aplikasi *anti-Malware*.
- 2** Tutup fungsi untuk sebarang sambungan seperti sambungan Bluetooth, Wi-Fi dan lain-lain sekiranya tidak digunakan dan tutup fungsi lokasi.
- 3** Penggunaan kata laluan, penguncian skrin dan penguncian kad SIM yang digunakan.
- 4** Penggunaan teknologi VPN (*Virtual Private Network*) dalam capaian internet. Sambungan dan lalu lintas yang berlaku dengan persekitaran akan dienkriptkan atau disembunyikan dalam bentuk kod rahsia. Antaranya ada perkhidmatan VPN ini yang dikhususkan untuk sistem Android seperti perkhidmatan oleh *Private Internet Access* - <http://www.privateinternetaccess.com>.
- 5** Dalam sistem Android ini, terdapat aplikasi yang terus dipasangkan ke dalam sistem komputer tanpa kebenaran dan sebagainya bila disambung ke internet. Jadi, perlu dipasang dalamnya aplikasi yang mengurus kebenaran pemasangan mana-mana aplikasi komputer seperti aplikasi XPrivacy dan lain-lain.
- 6** Pastikan sistem kamera yang terdapat dalam sistem Android dinyahaktifkan secara lalai dengan menggunakan konfigurasi sedia ada atau aplikasi pihak ketiga seperti aplikasi CameraBlock dan lain-lain. Sistem kamera ini mudah untuk dikompromi oleh pihak yang tidak bertanggung jawab untuk mencerooboh masuk ke dalam sistem komputer berasaskan Android.
- 7** Penggunaan aplikasi enkripsi untuk menghantar dan menerima mesej teks menerusi sistem pesanan ringkas seperti aplikasi TextSecure dan lain-lain.
- 8** Penggunaan aplikasi enkripsi untuk sebarang aktiviti perbualan dan panggilan telefon seperti aplikasi RedPhone dan lain-lain.
- 9** Sistem komputer berasaskan Android biasanya bersepadu dengan sistem atau aplikasi Google yang mudah dicapai menerusi internet. Jadi, boleh hilangkan apa sahaja mana-mana akaun aplikasi Google yang terdapat dalam komputer tablet atau telefon pintar yang berasaskan sistem Android.