Amalan Terbaik Keselamatan PC

- Pasang Penampal (patch)
    - Dibangunkan bagi mengatasi kelemahan atau pepijat yang ditemui selepas Sistem Operasi (OS) terbaru dikeluarkan. Kebanyakan kelemahan membabitkan Windows. Contohnya versi asal XP dinaiktaraf kepada XP Service Pack 2. Dilakukan melalui fungsi Auto Updates atau laman Microsoft http://windowsupdate.microsoft.com. Satu lagi kaedah iaitu melalui Version Tracker untuk mengimbas sistem sekaligus menjejaki kemaskini perisian-perisian berkenaan
- Gunakan Firewall
    - Perisian atau peranti firewall yang digunakan untuk mengawal akses keluar masuk PC dan maklumat menerusi internet. Ia boleh menyekat dan mengizinkan data yang tertentu sahaja melepasinya. Contoh Firewall percuma seperti ZoneLabs, Kerio atau Sygate dan dipasang pada PC masing-masing. Peranti firewall pula dipasang pada sambungan internet. Contoh vendor yang mengelurkan peranti firewall iailah Linksys, Netgear dan D-Link.
- Gunakan Antivirus
    - Penting untuk melindungi sistem daripada jangkitan virus yang merebak melalui e-mel atau internet. Sekurang-kurangnya antivirus yang percuma dan menawarkan cirri-ciri asas. Antivirus ini perlu dikonfigurasi bagi memastikan pengemaskinian dan pengimbasan menyeluruh secara berkala. Contoh Antivirus percuma iaitu AVG, AvitVir, Avast, Portable Antivirus dan lain-lain. Manakala yang terdapat dipasaran pula seperti Kaspersky, Norton, PC-Cilin dan lain-lain.
- Pasang Antispyware
    - Pakej antisypyware perlu dipasang bagi menangani spyware, adware dan program jahat yang lain (malware). Contoh perisian percuma iaitu Spybot Search and Destroy dan MWAV. Microsoft AntiSpyware juga boleh digunakan. Browser seperti Mozilla Firefox juga boleh dijadikan satu alternatif bagi menangani gangguan spyware dan iklan pop-up.
- Kenalpasti Penipuan
    - Muslihat atau penipuan alam siber biasa berlaku melalui e-mel atau telefon yang meminta supaya seseorang menyerahkan kata laluan atau data yang penting. Kerap menggunakan e-mel dan tapak web palsu sebagai taktik dan menggunkan teknik mengumpan (phishing). Biasanya emel yang dihantar kononya dari bank atau syarikat kewangan dan terdapat pautan untuk diklik atau no.telefon untuk dihubungi. Jangan dilayan e-mel berkenaan dan laporkan kepada pihak terbabit jika biasa menerima e-mel atau laman web yang dirasakan palsu.
- Kata Laluan Kukuh
    - Kata laluan yang kukuh dapat melindungi sistem yang digunakan. Gunakan sekurang-kurangnya 8 aksara dan kombinasi huruf, nombor dan special character. Perisian seperti KeePass boleh digunakan bagi menyimpan katalaluan yang berbeza untuk perkhidmatan yang berbeza. Kita hanya perlu mengingat satu kata laluan sahaja bagi membuka koleksi katalaluan.
- Teknologi Enkripsi

    - Penggunaan teknik enkripsi adalah satu lagi langkah keselamatan bagi memastikan kata laluan bukan hanya disorok tetapi yang penting tidak boleh difahami. Perisian seperti TrueCrypt adalah untuk mencipta pemacu maya sekaligus melindungi fail dengan efektif
- Penyimpanan Data
    - Simpanan (backup) data adalah langkah proaktif bagi melindungi maklumat sebelum terjejas oleh virus. Rutin penyimpanan yang sistemetik perlu diamalkan bagi kebolehsediaan data jika berlaku kehilangan atau kecurian PC. Perlu juga dilindungi dengan kata laluan atau dienkripsi bagi mendapatkan perlindungan yang efektif.