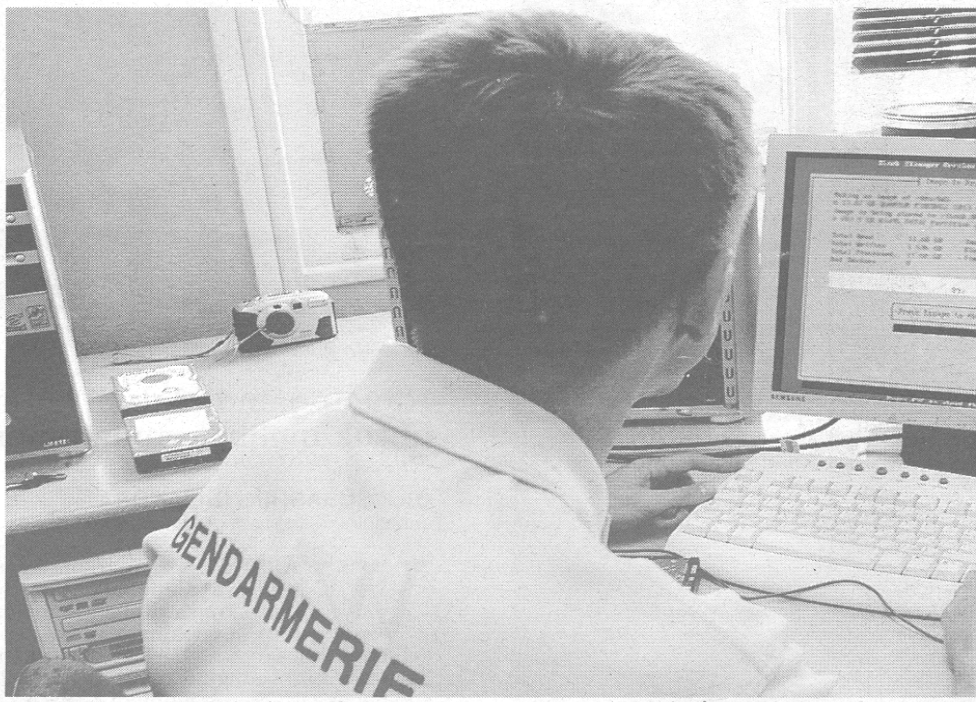
Mengurangkan ancaman sistem komputer

Anda pastinya tidak mahu sistem komputer anda dijangkiti virus, serangan penggodam, penipuan dan sebagainya. Cegah ia sebelum terkena!

Oleh KHAIRUL ANUAR ABD. RAHMAN
rencana@kosmo.com.my



KOMPUTER yang terjejas akibat ancaman virus dan sebagainya menyebabkan berlakuny terlibat untuk memperbaikinya.

TAHUKAH anda, selain menggunakan perisian antivirus dan mengemaskini antivirus, terdapat beberapa cara lagi yang boleh anda lakukan untuk mengurangkan risiko ancaman sistem komputer?

Kata orang, mencegah lebih baik daripada mengubati. Ikutilah beberapa langkah ini untuk mengelakkan pengeluaran wang yang tidak perlu di kemudian hari.

● Gunakan *firewall*. *Firewall* atau dinding api menghalang akses kepada komputer melalui rangkaian, sama ada internet mahupun rangkaian setempat. Dengan menutup sesebuah *port* pada komputer dari sambungan luar, ia dapat mengurangkan risiko serangan. *Firewall* terdapat dalam bentuk perisian dan juga perkakasan. Perisian *firewall* seperti BlackICE dan ZoneAlarm mampu memberikan perlindungan buat pengguna rumah.

● Amalkan penggunaan e-mel dan pelayaran internet yang selamat. Kebanyakan virus adalah berjangkit melalui e-mel. Virus lazimnya memasuki peti e-mel sebagai kepilan yang dihantar oleh rakan. Jangan terlalu bergantung kepada antivirus. Ada ketikanya, virus yang baru tidak dapat dikesan oleh perisian antivirus. Oleh itu, sekiranya anda menerima e-mel yang agak menyangsikan, jangan buka dan buang ia serta-merta!.

● Lindungi sambungan wayarles. Sambungan wayarles atau WiFi anda di rumah harus dilindungi daripada ancaman pengguna 'haram' yang turut boleh menceroboh sistem komputer anda. Baca aturan dan arahan pada manual yang didatangkan sekali dengan unit AP (*Access Point*) anda.

● Jangan berikan nombor PIN atau kata laluan melalui e-mel. *Phishing* merupakan aktiviti penipuan yang menjadikan internet sebagai mediumnya. Si penipu akan menghantar e-mel yang kelihatannya dari laman web yang dipercayai seperti bank, penyedia khidmat telefon selular dan sebagainya. Lazimnya, sindiket ini akan meminta pengguna mengemaskini butiran peribadi dan meminta anda mengklik pada pautan yang kemudiannya memperlihatkan laman web yang saling tidak tumpah seperti laman web yang asli. Namun, ia sebenarnya tidak lebih dari sebuah perangkap untuk mendapatkan segala butiran anda.

● Sering kemaskini sistem operasi dan perisian. Saban hari ada saja kepincangan atau 'jalan belakang' yang dijumpai penggodam.

● Pilih kata laluan yang unik dan jangan kongsikannya! Kata laluan seperti *admin, password, default, password123* dan *default123* merupakan kata laluan yang paling banyak digunakan di dunia. Jangan gunakan kata laluan ini kerana sesiapa sahaja boleh mencubanya. Gunakan kata laluan yang sukar diteka seperti nombor plet kereta, nama isteri atau nama anak. Kata laluan yang baik seharusnya mengandungi kombinasi abjad, nombor dan karektor (seperti *@&#).

● Buat salinan fail penting anda. Salinan atau *backup* merupakan langkah terbaik untuk menangani sebarang insiden yang tidak diingini. Terdapat pelbagai cara untuk melakukan *backup* seperti menyalinkan ke dalam CD-RW atau ke dalam cakera keras *external*.

● Nyahaktifkan ciri yang tidak diperlukan. Komputer lazimnya didatangkan dengan aturan yang sama. Ciri seperti perkongsian fail dan pencetak hanya mengundang penggodam, melainkan anda tahu apa yang anda lakukan dan berada dalam perlindungan *firewall*.

● Elakkan menggunakan perisian yang tidak selamat. Perisian percuma atau *freeware* seperti IM (pesanan segera) dan perisian muat turun muzik sering menarik perhatian kita. *Freeware* kadang kala didatangkan dengan *Adware* dan *Spyware* yang mengesan pergerakan pengguna di ruang siber dan melaporkannya kepada laman di internet tentang apa yang anda layari. Untuk mengetahui sekiranya komputer anda telah dimasuki program ini, anda boleh memuat turun perisian *Ad-Aware* di *www.lavasoftusa.com* atau *SpyBot Search & Destroy* di *www.safer-networking.org*.

● Jangan simpan maklumat sulit bersifat kritikal. Maklumat penting seperti nombor PIN ATM dan nombor kad kredit tidak sepatutnya disimpan di dalam komputer. Sekiranya komputer anda diceroboh, maklumat seperti ini boleh digunakan oleh mereka yang tidak diingini.

● Awas ketika membeli barangan secara dalam talian. Pastikan ciri memeriksa sijil dan maklumkan sekiranya sijil sesebuah laman web itu telah tamat tempoh pada pelayar internet anda diaktifkan. Ini dapat menggelakkan maklumat kad kredit anda daripada jatuh ke tangan pihak yang tidak bertanggungjawab.

● Sekiranya anda mengesyaki telah menjadi mangsa penipuan internet, laporkannya kepada MyCERT di *http://www.mycert.org.my*. MyCERT atau *Malaysian Computer Emergency Response Team* merupakan pihak yang menerima laporan berkaitan dengan insiden yang melibatkan komputer dan teknologi maklumat.