PENGURUSAN KATALALUAN

PANDUAN MELINDUNGI KATA LALUAN

1. Rahsiakan katalaluan anda dari orang lain walaupun kepada orang yang rapat dengan anda. Adalah diingatkan katalaluan anda adalah rahsia.

2. Jangan beritahu katalaluan anda secara lisan mahupun secara elektronik. Walaupun memberi hanya bayangan kepada katalaluan anda kepada orang lain, perbuatan ini juga akan membenarkan orang lain meneka katalaluan anda.

3. Jangan rakamkan *(record)* secara online katalaluan anda. Merakamkan katalaluan di PC adalah sama bahayanya dengan merakamkannnya ketika 'off-line' di mana orang lain boleh mencari dan mendapatkan katalaluan anda dari PC yang anda tinggalkan walaupun seketika. Menggunakan 'screen saver' yang menggunakan katalaluan mungkin dapat melindungi katalaluan tetapi penggunaannya tidak digalakkan.

4. Jangan menulis katalaluan anda di atas kertas, di dalam buku, diari atau di mana-mana yang boleh dijumpai dan dibaca oleh orang lain. Cara yang paling mudah dan selamat sekali ialah menghafal katalaluan anda.

5. Jangan biarkan orang lain berada berdekatan dengan anda ketika anda sedang menulis (menaip) atau memasukkan katalaluan. Orang lain mungkin dapat melihat gerak tangan anda ketika memasukkan (menaip) katalaluan. Jika rakan anda berada berdekatan dengan anda, anda boleh menyuruhnya berada jauh sedikit supaya dia tidak dapat melihat katalaluan yang ingin anda masukkan.

6. Jangan terlalu cepat memberikan maklumat yang berkaitan dengan katalaluan jika diminta. Siasat dahulu orang yang meminta maklumat berkenaan katalaluan anda

PERKARA YANG TIDAK PATUT DILAKUKAN KETIKA MEMILIH KATALALUAN

1. Jangan menggunakan *userId* atau *username* sebagai katalaluan walaupun dengan menambahkan beberapa patah perkataan lain. Pengguna gemar menggunakan katalaluan yang hampir-hampir sama dengan *userId* atau *username* kerana ia mudah diingat. Sebenarnya ia akan memudahkan lagi orang lain meneka katalaluan anda.

2. Jangan menggunakan perkataan yang diambil dari kamus dalam Bahasa Inggeris atau apa bahasa sekalipun. Program pemecah katalaluan seperti *L0phtCrack*, *CrackerJack* dan *John the Ripper* mempunyai keupayaan untuk meneka katalaluan dengan pantas.

3. Jangan membina katalaluan yang terdiri hanya huruf-huruf atau angka-angka sahaja atau huruf-huruf yang sama contohnya "ssssss". Ini akan memudahkan lagi orang lain memecah katalaluan dengan mengambil masa yang singkat.

4. Jangan menggunakan perkataan yang mudah diteka atau yang selalu digunakan seperti memilih perkataan "Sayang" atau "LoveYou".

5. Jangan menggunakan perkataan yang ada kaitan dengan anda contohnya tarikh harijadi, nama ahli keluarga atau nombor pendaftaran kereta.

6. Jangan menggunakan huruf-huruf dari corak *(paterns)* keyboard seperti "qwerty" atau huruf-huruf yang berganda seperti "aaabbbcc".

TIPS KETIKA MEMILIH KATALALUAN

1. Gunakan 8 huruf ke atas sebagai katalaluan. Jumlah huruf yang sedikit memudahkan lagi katalaluan dipecah *(cracked)*.

2. Gunakan campuran huruf kecil, huruf besar dan angka sebagai katalaluan.

3. Tukarkan katalaluan setiap 3 bulan atau kurang. Jadikan ia sebagai satu tabiat.

MENGHALANG E-MEL TIDAK DIUNDANG

Kotak mel anda dipenuhi dengan mel elektronik (e-mel). Ia bukannya dipenuhi dengan kandungan e-mel yang marahkan anda kerana sesuatu perkara atau bengang dengan sikap anda. Sebenarnya ia dipenuhi dengan e-mel yang tidak diundang dari pihak atau orang yang tidak anda kenali, malah kadang-kadang ada e-mel robot (e-mel yang dihantar secara automatik oleh pelayan komputer).

Inilah yang dikatakan kegiatan 'spamming' iaitu e-mel yang datangnya tanpa diundang dan tidak diperlukan oleh anda.

Satu kajian yang dibuat oleh GartnerGroup, badan penyelidik di Stamford, Connecticut Amerika Syarikat mendapati bahawa 90 peratus pengguna internet didatangi e-mel tidak diundang secara mingguan dan lebih 50 peratus daripadanya secara harian.

Pengguna yang terselamat dari fenomena ini hanyalah pengguna yang telah mengambil langkah yang ketat dengan meletakkan perisian pertahanan *anti-spamming* dalam aplikasi e-mel mereka.

Di sini dipaparkan beberapa langkah bagi melawan balik kegiatan penghantaran kandungan e-mel yang tidak diundang ini:

1. Jangan sesekali menjawab e-mel yang tidak diundang. Jika anda menjawab balik, maka pihak terbabit akan mendapat kepastian bahawa alamat e-mel anda adalah sah. Pastinya anda akan dipenuhi dengan e-mel yang bertambah banyak.

2. Daftar atau langganilah akaun e-mel berasaskan web. Gunakan alamat ini sebagai alamat yang 'dibuang' sekiranya anda telah tersenarai dalam senarai pihak berkenaan.

3. Hantarkan e-mel yang tidak diundang kepada SpamRecycling Center (www.spamrecycle.com). Pusat ini akan panjangkan e-mel anda kepada pihak berkuasa bagi memeriksa kegiatan yang tidak bertanggungjawab ini. Pihak JARING juga menyediakan alamat bagi menolong anda mengatasi masalah ini dengan menghantar kandungan e-mel berkenaan kepada abuse@jaring.my. Antara kategori kandungan e-mel jenis ini ialah e-mel yang tidak berfaedah secara kerap.

4. Ada beberapa pihak lain yang bertugas menangani masalah ini. Salah satunya ialah SpamCop (www.spamcop.net). Anda simpan kandungan e-mel tersebut, dan kemudian pihak SpamCop akan menghubungi Penyedia Perkhidmatan Internet (ISP) yang digunakan oleh pihak spamming sebagai tapak kegiatan mereka. Pihak lain ialah seperti Junkbusters (www.junkbusters.com) dan Network Abuse Clearing house (www.abuse.net).

5. Gunakan penapis e-mel tidak diundang terkini. Contohnya perpustakaan perisian ZDNet (www.hotfiles.com) ada menyediakan versi demo perisian berkenaan secara percuma dengan nama Spam Buster dan SpamEater.

6. Apabila anda menghantar e-mel kepada kumpulan perbincangan, letakkan perkataan seperti 'NOSPAM' kepada alamat e-mel balasan anda. Misalnya hizam@syarikatNOSPAM.net. Ahli-ahli perbincangan akan dapat mengesannya, tetapi tidak bagi pihak yang ingin menghantar e-mel tidak diundang itu.

7. Tanyakan pihak ISP anda berapa ramaikah kakitangan yang dikhususkan bagi mengesan kegiatan e-mel tidak diundang ini. Adalah elok jika ISP anda menyediakan sekurang-kurangnya seorang kakitangan bagi setiap 100,000 pelanggan. Jika tidak elok sekiranya anda tukar ISP.

8. Satu alamat e-mel yang baik ialah yang berakhir dengan .edu atau .gov. Menurut pihak Spambot (www.turnstep.com/Spambot), kumpulan penghantaran e-mel tidak diundang cuba elakkan alamat sebegini.