Abai maklumat untungkan penjenayah

Oleh SHAHARUDIN ISMAIL

KETIKA Akademi Fantasia musim keenam (AF6) menuju kemuncaknya, tersiar di akhbar kisah seorang imam di Arau, Perlis yang terpedaya dengan sindiket penipuan menerusi SMS AF6. Bagaimanapun nasib masih menyebelahi imam tersebut yang cepat tersedar dan hanya kehilangan RM240 sahaja.

Kisah ini adalah satu contoh bagaimana mudahnya maklumat diri seseorang boleh diperolehi pada masa kini. Sama ada kita sedar atau tidak, sebenarnya penjenayah boleh memperolehi pelbagai jenis maklumat diri kita dengan begitu mudah dan menggunakannya untuk sesuatu niat yang tidak baik (kebanyakan didorong oleh kewangan) seperti kes peras ugut dan penipuan.

Maklumat diri seperti tarikh kelahiran, nama, alamat, nombor telefon, nombor kad pengenalan, nombor lesen memandu, nombor kad pelajar, nama pengguna dan kata laluan akaun Internet, nombor dan kata laluan perbankan Internet, maklumat kad bank dan kad kredit.

Semua maklumat ini sebenarnya boleh diperolehi dengan mudah melalui sijil kelahiran, lesen memandu, rekod kesihatan, rekod pekerjaan, rekod kredit, transkrip kolej, pasport, e-mel, surat-surat yang diterima, bil elektrik, bil telefon, bil air, polisi insurans, penyata akaun bank, penyata kad kredit dan sebagainya.

Maklumat ini yang kebanyakannya disimpan di rumah dan pejabat juga boleh diperolehi dari dalam beg duit, beg tangan, bakul sampah, komputer, Internet dan juga kabinet fail.

Sejak beberapa tahun lalu, kes-kes kecurian maklumat diri semakin meningkat. *Identity Theft New Survey & Trend Report* telah menganggarkan 38 peratus atau kira-kira 14 juta warga dewasa Amerika Syarikat (AS) menjadi mangsa kecurian maklumat diri dalam tempoh Januari 2001 hingga pertengahan Mei 2003. Dalam tempoh yang sama, kumpulan mangsa ini juga telah kehilangan lebih kurang AS$3.8 bilion (RM14.4 bilion) bagi tujuan pembayaran yang bersabit daripada kes-kes penipuan ini.

Majalah *Communications* telah memberi amaran kepada pembacanya berkenaan peningkatan kes kecurian maklumat diri di AS sehingga menjadikannya jenayah yang sangat perlu diberi perhatian.

Pasukan Tindakbalas Kecemasan Komputer Malaysia (MyCERT) mengklasifikasikan kes-kes kecurian maklumat diri sebagai sebahagian daripada kegiatan penipuan siber.

MyCERT melaporkan bahawa terdapat peningkatan ketara dalam kegiatan penipuan siber, iaitu 364 kes pada tahun 2007 berbanding 287 kes pada tahun 2006, 149 kes (2005) dan 106 kes (2004).

Peningkatan ini adalah sangat ketara dan perlu diberi perhatian kerana bilangan kes penipuan di Malaysia adalah kurang daripada 30 kes setiap tahun di antara tahun 2000 hingga 2003. MyCERT juga menyatakan dalam empat (4) bulan pertama tahun 2008, sebanyak 124 kes telah dilaporkan berbanding 90 kes dalam tempoh yang sama pada tahun 2007 dan 86 kes dalam 2006.

Walaupun angka kes kecurian maklumat diri ini tidak serius berbanding AS, warga Malaysia masih perlu berwaspada kerana ia merupakan satu bentuk jenayah yang boleh menimbulkan impak kewangan ketara.

Perkembangan teknologi bukan hanya membawa kebaikan kepada masyarakat tetapi juga boleh membawa keburukan jika tidak digunakan dengan baik. Seperti contoh, perkembangan teknologi Internet telah memudahkan pelanggan perbankan Internet menjalankan urusan mereka tetapi dalam masa yang sama teknologi ini boleh digunakan oleh penjenayah untuk menjalankan kegiatan jahat mereka seperti mendapatkan maklumat diri mangsa yang kemudiannya digunakan untuk mencuri wang melalui perbankan Internet.

Maklumat

Kecurian ini boleh dilakukan walaupun penjenayah berada beribu-ribu kilometer jauhnya daripada mangsa. Pelbagai kaedah daripada penggunaan teknik konvensional hingga penggunaan teknologi yang canggih boleh digunakan oleh penjenayah dalam usaha mencuri maklumat peribadi seseorang.

Kaedah konvensional yang digunakan dalam mencuri maklumat peribadi adalah seperti tinjauan bahu (*shoulder surfing*), penggeledahan maklumat buangan (*dumpster diving*), mendengar perbualan telefon dan mencuri maklumat maklumat peribadi seperti nombor kad kredit dari dalam beg tangan yang dicuri atau diperolehi melalui kes ragut. Kecurian komputer juga salah satu kaedah kecurian maklumat peribadi yang membolehkan penjenayah mendapatkan maklumat peribadi daripada pangkalan data dalam cakera keras.

Kemajuan teknologi komputer dan Internet telah membolehkan maklumat terperinci mengenai pengguna dikumpul dan dikongsi pakai dengan lebih mu- dah. Maklumat peribadi lebih mudah diakses dan maklumat mengenai seseorang boleh didapati tanpa pengetahuannya.

Mereka boleh menggunakan teknik canggih seperti menggodam (*hacking*) dan menyalin pangkalan data dalam server, mengintip dalam rangkaian dan juga mengumpan (*phishing*).

CyberSecurity Malaysia pernah mengeluarkan 13 panduan untuk perbankan Internet selamat yang boleh diperolehi daripada laman web agensi berkenaan. Panduan ini perlu diamalkan supaya kita dapat melindungi maklumat peribadi.

Risiko kecurian maklumat peribadi boleh dikurangkan jika cadangan berikut diambil kira:

Sebelum memberi sebarang maklumat peribadi dalam talian, pastikan anda berurus niaga dengan syarikat yang sah. Anda perlu menentukan kesahihan syarikat yang anda berurusan sebelum membekalkan sebarang maklumat.

Manfaatkan ciri-ciri keselamatan seperti kata laluan dan lain-lain bagi tujuan menambah lapisan keselamatan. Lapisan keselamatan lain adalah menggunakan tanda perantaraan seperti kad pintar dan maklumat biometrik seperti cap jari dan pengecaman iris.

Ambil langkah berjaga-jaga semasa memberi maklumat dalam talian dengan menyemak polisi kerahsiaan laman web yang anda berurusan.

Lindungi komputer anda daripada serangan virus, cecacing, Trojan dan pengancam berbahaya lain dengan menggunakan perisian anti virus yang berlesen.

❐ **SHAHARUDIN ISMAIL ialah Pensyarah di Fakulti Sains dan Teknologi, Universiti Sains Islam Malaysia (USIM) yang kini melanjutkan pengajian di La Trobe University, Melbourne, Australia.**