

PERLINDUNGAN data merupakan suatu isu penting yang perlu dititikberatkan oleh para pengguna. Tidak ramai yang sedar bahawa data peribadi yang diberikan oleh mereka kepada pihak-pihak tertentu boleh disalahgunakan oleh pihak yang tidak bertanggungjawab. Di Malaysia, kes kecurian identiti dan penyalahgunaan data peribadi berada pada tahap yang membimbangkan kerana terdapat banyak kes yang telah berlaku. Namun begitu, undang-undang yang sedia ada tidak dapat memberikan perlindungan secara menyeluruh.

Secara umumnya, perlindungan data bertujuan untuk memastikan keselamatan terhadap maklumat yang telah kita berikan kepada pihak-pihak tertentu agar maklumat tersebut tidak disalahgunakan untuk kepentingan mereka. Contohnya, maklumat peribadi yang telah diberikan kepada bank untuk memohon kad kredit, maklumat kepada syarikat telekomunikasi untuk mendaftar perkhidmatan telekomunikasi ataupun maklumat peribadi yang diberikan melalui laman web seperti laman web jaringan sosial (facebook, myspace dan sebagainya).

Sebagai pengguna, kita perlu sedar bahawa isu perlindungan data ini tidak sewajarnya dipandang remeh kerana ia melibatkan penggunaan data peribadi seperti nama penuh, alamat rumah, alamat tempat kerja, nombor kad pengenalan, nombor telefon dan nombor kad kredit yang boleh digunakan oleh pihak yang mempunyai akses terhadap data tersebut tanpa mendapat keizinan terlebih dahulu untuk tujuan yang tidak diingini.

MASALAH YANG SERING DIKAITKAN DENGAN PERLINDUNGAN DATA

Antara masalah yang sering dikaitkan ialah penyalahgunaan data peribadi seperti:

■ Data peribadi dijual kepada pihak ketiga

Kita mungkin pernah menerima panggilan telefon, pesanan ringkas atau e-mel daripada syarikat yang menawarkan perkhidmatan atau produk tertentu. Sekiranya kita tidak mempunyai sebarang perhubungan rekod dengan syarikat tersebut, sudah tentu kita berasa curiga bagaimana maklumat tentang diri kita boleh diperolehi oleh mereka. Sebenarnya, syarikat ini merupakan pihak ketiga yang memperoleh data daripada institusi yang mempunyai data peribadi kita. Terdapat satu kes yang telah dilaporkan tentang senarai pangkalan data sebuah bank yang mengandungi lebih daripada satu juta senarai nama pelanggan, tempat tinggal, nombor telefon bimbit, jenis kad kredit yang dimiliki (classic, gold atau platinium), nombor kad pengenalan dan sebagainya yang dijual melalui iklan surat khabar dengan harga RM100 sahaja.

Bayangkan, senarai yang mengandungi data peribadi lebih daripada satu juta pelanggan dijual dengan harga RM100 sahaja. Ini bermakna harga bagi data peribadi untuk seorang pelanggan dijual dengan harga yang terlalu rendah. Keadaan seperti ini sangat membimbangkan kerana begitu mudah sekali data peribadi kita dijual kepada pihak ketiga sedangkan ia melibatkan data peribadi sulit yang perlu dilindungi.

Perkara seperti ini berlaku disebabkan oleh wujudnya pihak-pihak tertentu yang memerlukan data peribadi ini untuk kepentingan mereka seperti mendapatkan pelanggan baru bagi perniagaan mereka. Contohnya pihak yang terlibat dengan pemasaran produk akan menggunakan data peribadi itu untuk mempromosikan produk keluaran mereka.

Selain daripada itu, pangkalan data daripada syarikat kad kredit amat berguna kepada perniagaan kerana ia memaparkan corak pembelian seseorang individu. Contohnya, pemaju perumahan yang ingin menjual rumah kos tinggi akan menghubungi

individu-individu yang mempunyai corak perbelanjaan yang mewah.

Bagi mereka, sekiranya mereka mendapat maklum balas sebanyak lima hingga tujuh peratus daripada data peribadi yang diperolehi, ia merupakan satu pulangan yang baik.

■ Kecurian Identiti

Kecurian identiti merupakan satu ancaman yang serius kepada keselamatan diri kita kerana data peribadi yang dicuri boleh digunakan secara tidak sah oleh pihak lain. Data peribadi seperti tarikh lahir, nombor akaun bank, nombor kad kredit, kata laluan internet atau sebarang maklumat penting boleh digunakan oleh individu yang tidak amanah dengan sewenang-wenangnya. Ini mengakibatkan kita menanggung risiko kerugian kewangan.

TAKTIK YANG DIGUNAKAN UNTUK MENDAPATKAN MAKLUMAT

Kecurian identiti berlaku apabila pencuri identiti mendapatkan maklumat peribadi menggunakan pelbagai cara/ taktik:

- Mencuri dompet yang mengandungi kad pengenalan dan kad kredit.
- Mencuri surat yang mengandungi maklumat tentang bank, kad kredit, slip gaji dan cukai.
- Memperolehi kad pertukaran alamat agar semua surat dihantar ke alamat lain.
- Pecah masuk rumah untuk mendapatkan maklumat peribadi.
- Mencuri maklumat peribadi melalui internet.
- Menyamar sebagai wakil bank, penyedia perkhidmatan internet atau agensi kerajaan bagi mendapatkan maklumat

peribadi melalui telefon atau e-mel.

BAGAIMANA PENCURI IDENTITI MENGGUNAKAN MAKLUMAT PERIBADI YANG DIPEROLEHI

- Membuka akaun bank menggunakan nama anda dan menulis cek yang tidak sah daripada akaun itu.
- Menyamar sebagai diri anda di laman web jaringan sosial seperti facebook.
- Memalsukan cek dan mengeluarkan wang dalam akaun simpanan.
- Memohon perkhidmatan telefon atau perkhidmatan tanpa wayar atas nama anda.
- Memohon kad kredit baru menggunakan nama anda.
- Menambah bil utiliti yang perlu ditanggung oleh anda. Mungkin anda tidak nampak bil perbelanjaan tetapi kegagalan membayarnya akan memberi kesan terhadap reputasi kewangan anda.

Terdapat satu kes kecurian identiti dilaporkan dalam media baru-baru ini, iaitu seorang wanita berasa hairan apabila beliau sering menerima e-mel yang meminta untuk menambah beliau sebagai kawan pada profil di sebuah laman web jaringan sosial. Kebiasaannya, wanita tersebut tidak akan menambah keahlian bagi orang yang tidak dikenali dalam profilnya. Oleh itu beliau berasa terkejut apabila mendapati ramai orang yang tidak dikenali mengatakan bahawa mereka mengenali beliau. Mereka mengatakan bahawa wanita tersebut telah menambah mereka sebagai kawan di laman web jaringan sosial yang lain. Setelah beliau melayari laman web tersebut, beliau mendapati bahawa ada orang lain yang telah membuat satu profil palsu menggunakan

gambar serta maklumat peribadinya. Apabila beliau menghubungi orang tersebut agar menutup akaun profil itu, orang yang menyamar itu telah meletakkan profil palsu kepada private – hanya boleh dilihat oleh orang yang dipilih sahaja.

Ini merupakan satu bentuk kecurian identiti yang amat serius. Penyamar boleh menghubungi kawan-kawan anda dan menipu bagi mendapatkan wang daripada mereka. Penyamar juga boleh meletakkan sebarang kenyataan tidak baik untuk memusnahkan reputasi anda atau meletakkan pautan muat turun perisian yang mengandungi virus pada profil kawan-kawan anda.

Sekiranya keadaan seperti ini berlaku, anda dinasihatkan agar menghubungi Cybersecurity Malaysia (agensi kerajaan yang mempunyai kepakaran dalam bidang keselamatan ruang siber) untuk mendapatkan khidmat dengan menghantar emel ke cyber999@cybersecurity.my. Mereka akan membantu mangsa membuktikan bahawa identiti mangsa tersebut telah dicuri dan akan terus menghubungi laman web jaringan sosial yang berkenaan supaya menutup profil palsu tersebut. Cybersecurity juga boleh merujuk kes kepada pihak polis untuk tindakan selanjutnya.

CARA-CARA MELINDUNGI DATA PERIBADI

- Memastikan surat-surat penting diuruskan dengan baik. Pastikan surat yang hendak dikirim diletakkan di dalam peti pos dan pastikan surat yang diterima diambil terus daripada peti surat.
- Menyimpan maklumat peribadi di tempat yang selamat seperti laci yang berkunci.
- Melindungi maklumat sulit dalam komputer dengan kata laluan yang mengandungi kombinasi nombor dan huruf. Elakkan daripada menggunakan kombinasi kata laluan yang mudah seperti tarikh lahir, nombor kad pengenalan dan sebagainya.
- Jangan memberikan maklumat peribadi melalui e-mel atau laman web kecuali jika anda benar-benar pasti bahawa penerima maklumat tersebut boleh dipercayai.
- Sebelum memberikan data peribadi dalam laman web tertentu, pastikan laman web tersebut adalah selamat iaitu laman web yang mempunyai ciri-ciri keselamatan yang dapat memberi perlindungan maklumat daripada dicuri ketika transmisi. Alamat laman web yang bermula dengan "https" menandakan laman web tersebut dalam kedudukan yang selamat.
- Sekiranya mempunyai talian internet di rumah, semak dengan penyedia perkhidmatan tentang tahap keselamatan talian tersebut. Selidik apakah langkah-langkah yang perlu diambil untuk melindungi komputer dan data yang terdapat di dalamnya.
- Sebelum membuang dokumen penting seperti penyata bank dan cek, koyakkan terlebih dahulu. Kad kredit yang telah luput juga perlu dipotong. Ini untuk mengelakkan daripada seseorang mendapatkan maklumat daripada kad kredit tersebut.

– Buletin Pengguna, Nov, 2009.



AWASI KESELAMATAN DATA PERIBADI