ڤرساتوان بڠک بروني
THE BRUNEI ASSOCIATION OF BANKS

APA ITU JENAYAH SIBER?

Jenayah siber merupakan satu jenayah yang berkembang cepat dengan skop yang sangat meluas. Ianya merangkumi apajua perbuatan jenayah yang melibatkan penggunaan computer dan rangkaian, termasuk jenayah yang dilakukan melalui Internet. Sebagai contoh, penipuan dalam talian adalah dianggap sebagai jenayah siber, begitu juga dengan penipuan telepemasaran.

Di Negara Brunei Darussalam, "trend" umum jenayah siber telahpun meningkat, dimana kebanyakkan jenayah yang dilaporkan oleh pihak media melibatkan penggunaan media sosial, terutamanya berkaitan dengan jenayah kewangan.

Sabitan Jenayah Siber Pertama

Sabitan jenayah siber pertama di Negara Brunei Darussalam melibatkan penggunaan tanpa kebenaran ke dalam sambungan Internet Tanpa Wayar dan penggunaan nombor kad kredit yang dicuri untuk membuat pembelian melalui talian yang bernilai BND2,720.

Yang tertuduh bertindak memalsukan dirinya sebagai pemilik laman sesawang dan berjaya mendapatkan siri pembelian dalam talian yang diluluskan dari pemilik laman sesawang. Beliau akhirnya telah ditangkap dan dihukum penjara selama enam bulan atas kesalahan pertama dan menerima hukuman tambahan 22.5 bulan penjara bagi pembelian menggunaakan kad kredit yang dicuri, yang telah dijalankan secara serentak.

Mengapa kita perlu tahu tentang Jenayah Siber

Walaupun penggunaan teknologi semakin mudah dan meningkatkan cara untuk kita berkongsi maklumat dalam menjalankan kehidupan seharian kita, kita tidak dapat menafikan setiap kali kita menggunakan Internet untuk berkomunikasi dan membuat transaksi kewangan, kita terdedah kepada tahap kelemahan yang tertentu.

Realitinya adalah semua individu dan organisasi yang mempunyai komputer atau telefon yang disambungkan kepada rangkaian atau Internet berkemungkinan terdedah kepada risiko. Jika kita tidak mengambil langkah berjaga-jaga, banyak kemungkinan rangkaian boleh diakses and disalah guna oleh penjenayah siber dari mana-mana pelusuk dunia.

Perkara-perkara yang perlu diambil perhatian

1. E-mel Spam dan Short Messaging Service (SMS)

Spam adalah elektronik mel yang tidak berkenaan atau e-mel yang tidak diminta, dan biasanya bertujuan untuk mempromosikan tawaran menarik yang dihantar kepada sebilangan besar pengguna dengan tujuan mengiklanan, "phishing" iaitu aktiviti menipu pemegang akaun dalam talian maklumat kewangan dengan menyamar sebagai syarikat yang sah) dan menyebarkan "malwarei iaitu perisian yang bertujuan untuk merosakkan atau melumpuhkan komputer dan sistem komputer.

Terdapat peningkatan yang ketara dan jumlah spam yang dihantar melalui e-mel pada masa kini selaku halangan kemasukkan ke dalam internet dan operasi yang rendah. Kebanyakkan langkah-langkah terhadap sekuriti e-mel tidak menganggap e-mel spam tersebut sebagai satu ancaman dan biasanya tidak menghalangnya dari memasuki "inbox".

2. Penipuan

Ada pelbagai bentuk penipuan yang berbeza. Penipuan biasanya melibatkan penerimaan panggilan yang diterima daripada seseorang, dimana mangsa akan dimaklumkan bahawa mangsa telah pun memenangi hadiah besar dalam pertandingan loteri. Pemanggil akan cuba untuk memancing minat mangsa dengan mengatakan bahawa "Awda tidak perlu khuatir mengenai persaraan" atau "Awda sekarang boleh mendapatkan rumah yang besar untuk keluarga". Walaubagaimanapun, untuk mendapatkan duit hadiah, mangsa dikehendaki untuk membayar beberapa jenis 'yuran pemprosesan'. Beberapa transaksi (kerapnya melalui penghantaran wang) perlulah dilakukan sebelum mangsa menyedari yang mereka telah ditipu.

Ada diantara penipuan yang dibuat menggunakan temujanji bagi mengumpan mangsa-mangsa mereka. Mereka membuat profil palsu pada laman media social dan menyamar diri sebagai orang-orang yang menarik. Mereka terlebih dahulu akan mendapatkan kepercayaan mangsa dengan memulakan hubungan. Sesetengah akan meminta bantuan kewangan daripada mangsa dan akan menghilang diri sebaik sahaja mereka medapatkan wang mangsa. Beberapa skim lain yang rumit melibatkan penyamaran seorang lelaki yang bujang (yang selalunya mempunyai banyak kemewahan) yang telah jatuh cinta dengan mangsa (kerapnya wanita pertengahan umur, wanita bujang). Mereka mendakwa bahawa mereka telah menghantar 'hadiah' yang kemudiannya ditahan di tempat transit dalam perjalanan menuju ketempat mangsa. "Pegawai kastam" kemudian akan menghubungi dan menuntut supaya mangsa membayar 'yuran pemprosesan' untuk melepaskan hadiah berkenaan.

3. Penggodaman

Penggodam mendapatkan maklumat peribadi di dalam internet melalui pelbagai cara rangkaian sosial dan e-mel. Maklumat sensitif boleh didapatkan, contohnya lokasi awda, maklumat mengenai percutian awda, maklumat anak-anak awda dan dalam kes yang paling serious adalah melibatkan maklumat kewangan awda. Dalam sesetengah kes, penggodam akan membuat akaun palsu di dalam laman rangkaian sosial untuk menyamar sebagai awda untuk menipu rakan karib dan keluarga awda.

Cara-cara untuk melindungi dari Jenayah Siber

a. Gunakan perisian anti-virus

Virus dan perisian berniat jahat dengan mudah boleh dimasukkan ke dalam lampiran e-mel, muat turun fail atau laman sesawang. Awda perlulah bersikap bertanggungjawab dan berwaspada akan perkara yang awda muat turun, layari dan memasuki. Dengan adanya pemasangan anti-malware atau perisian anti-virus ianya akan mengurangkan kemungkinan komputer awda dari dijangkiti melalui amaran keatas potensi ancaman.

b. Tidak ambil peduli 'pop-ups'

‘Pop-ups’ boleh mengandungi perisian berniat jahat yang boleh memperdayakan pengguna untuk mengesahkan sesuatu. Sebaik sahaja awda melakukan muat turun, ada pemasangan yang dibuat secara sembunyi dari perisian yang berniat jahat. Ini dikenali sebagai muat turun ‘drive-by’.

c. Pengesahan dua faktor

Sekiranya e-mel atau perkhidmatan media social menawarkan awda pengesahan dua faktor, adalah disyorkan untuk mendapatkan cara tersebut. Di samping memasukkan kata laluan awda, ini bermakna awda juga akan diminta untuk memasukkan kod pengesahan yang dihantar melalui SMS ke telefon awda. Penggodam mungkin dapat memecahkan kata laluan awda, tetapi tanpa kod pengesahan yang unik dan sementara, mereka tidak akan dapat mengakses akaun awda.

d. Apabila membeli-belah dalam talian, gunakan laman sesawang yang selamat.

Sentiasa pastikan bahawa simbol ‘kunci manga yang dikunci’ atau 'Kunci yang tak pecah’ada di skrin pelayar awda sebelum memasukkan butiran kad kredit awda. Sebagai tambahan, permulaan alamat laman sesawang akan berubah daripada 'http' kepada 'https' untuk menunjukkan sambungan yang selamat. Berhati-hati dengan alamat laman sesawang yang tertukar kembali ke ‘http’ sebaik sahaja awda telah masuk kedalam laman sesawang tersebut.

e. Cara-cara lain untuk mengelakkan daripada menjadi mangsa jenayah Siber adalah seperti berikut:

•Pasangkan penyulitan perisian.

•Banyakkan membaca dan tingkatkan kesedaran awda tentang penipuan supaya anda boleh mengelakkan dari mereka.

•Perhatikan aktiviti-aktiviti yang ada didalam komputer anak-anak awda.

- Berhati-hati dengan orang luar (daripada mana-mana jantina) yang meminta untuk ‘video chat’ dengan awda kerana ini boleh dirakam dan digunakan sebagai peras ugut kepada awda.

•Gunakan kata-laluan selamat yang tidak mudah diteka (Jangan gunakan '12345', 'password', dll), dan sentiasa ditukar.

•Pastikan perisian sentiasa dikemas kini dan terkini.

•Jangan gunakan perisian cetak rompak kerana ia mungkin mengandungi virus.

Berhati-hati – lakukan siasatan awda sendiri untuk mengetahui lebih lanjut. Muat turun aplikasi "AMBD" pada telefon pintar awda untuk mengetahui lebih lanjut tentang jenis penipuan kewangan.
Berwaspada–kerana tidak ada perkara yang menawarkan wang percuma.
Dapatkan Nasihat-hubungi pihak berkuasa tempatan jika awda rasa curiga.

Bagaimana hendak melaporkan jika awda adalah mangsa

Mangsa atau mana-mana individu yang telah mensyaki bahawa mereka mungkin telah dijadikan sasaran dalam satu cubaan penipuan, bolehlah:

1. Laporkan kepada pihak polis

Sila laporkan kepada balai polis yang berhampiran dan pastikan awda memberikan pihak polis maklumat sebanyak yang mungkin.

2. Hubungi Bank awda

Jika awda mensyaki yang akaun awda atau fasiliti kewangan awda telah dikompromi.