

7 KIAM MENGHINDARI PEMBOBOLAN REKENING (Himbauan Kepada Masyarakat dan Keterangan Pers)

Maraknya kejadian pembobolan rekening melalui eksploitasi kelemahan sistem layanan ATM dan juga SMS serta Internet banking menunjukkan semakin canggihnya para penjahat cyber. Pihak perbankan harus memiliki sistem pengamanan yang kuat dan terus ditingkatkan kemampuannya dari waktu ke waktu untukantisipasi berbagai jenis upaya kejahatan yang terus berubah dan berkembang.

Meskipun demikian, agar terhindar dari tindak kriminal, diperlukan juga peran aktif nasabah. Karena di dalam dunia keamanan dikenal istilah "your security is my security". Semua pihak harus melakukan peningkatan pengetahuan dan pemahaman bahwa di dalam pemanfaatan berbagai macam layanan yang berbasis teknologi, selain memudahkan juga terdapat resiko yang harus diwaspadai.

Berikut ini adalah 7 kiat untuk menghindari aksi pembobolan rekening ini:

1. Tak Kenal Maka Tak Sayang

Kenali layanan yang digunakan dan cermati bagaimana cara kerja teknologinya serta pahami aturan serta prosedur yang diterapkan terutama di dalam aspek pengamanan. Bank memiliki banyak produk dan layanan, sudah sepatutnya nasabah memahami dan dapat membedakan karakteristiknya. Contoh layanan SMS/mobile banking dan Internet banking pada prinsipnya adalah perluasan dari layanan ATM namun dengan fitur yang lebih terbatas dibandingkan ATM. Artinya, tidak semua fitur yang tersedia di ATM (misalnya ganti PIN) bisa digunakan pula di SMS/mobile banking atau Internet banking.

Nasabah juga perlu mengetahui, bahwa untuk dapat menggunakan SMS/mobile banking dan Internet banking, terlebih dahulu harus memiliki kartu ATM dan PIN yang nanti akan digunakan untuk aktivasi/mendaftar. Bila nasabah telah paham kondisi ini, maka ybs. dapat memilih untuk menggunakan atau tidak menggunakan layanan tersebut sesuai kebutuhannya. Sebab tidak semua orang memanfaatkan online banking bahkan kartu ATM pun belum tentu digunakan. Sementara sebagian bank, terutama yang sudah online seolah menerapkan keharusan setiap nasabah untuk memiliki kartu ATM.

Setelah memahami karakteristik layanan, maka selanjutnya nasabah juga perlu mengetahui cara kerja teknologi yang bekerja di balik layanan tersebut. Edukasi semacam ini seharusnya menjadi tanggung jawab bank dan atau pihak penyedia teknologi seperti misalnya operator selular dan provider Internet. Yang paling penting di dalam edukasi ini adalah untuk menanamkan pemahaman dan disiplin kepada nasabah prosedur pemanfaatan layanan dan teknologi yang benar, mengenali kelemahannya dan juga sekaligus tata cara pengamanannya. Dengan memahami resiko, nasabah akan lebih waspada.

Yang paling penting bagi nasabah adalah, tidak ada keharusan untuk memanfaatkan semua layanan, fitur dan teknologi yang ditawarkan. Sesuaikan dengan kebutuhan anda, manakah yang paling mudah (dikuasai) dan paling nyaman untuk digunakan di dalam menunjang aktivitas transaksi.

*) catatan: anda punya pilihan untuk memilih bank dan jenis produk layanannya yang paling sesuai dengan kebutuhan. Semua bank masih tetap memiliki layanan teller konvensional dan punya cabang hingga ke pelosok, terutama beberapa bank nasional maupun bank daerah milik pemerintah.

2. Mengetahui Jenis Kartu Transaksi

Khusus untuk layanan yang menggunakan kartu sebagai media, ATM, debit, voucher elektronik, kartu kredit, dlsb. perlu diketahui jenis kartu yang dipakai. Pada prinsipnya saat ini ada 2 jenis kartu yaitu:

Magnetic stripe card, mengikuti standar ISO/IEC untuk ukuran, bentuk, karakteristik bahan magnetik yang digunakan, penempatan jalur pita magnetik, hingga format penyimpanan data. Prinsipnya kartu jenis ini menyimpan data di dalam pita magnetik yang kemudian dapat dibaca ulang menggunakan alat yang memiliki head pembaca seperti di dalam perangkat tape recorder, dengan cara digesekkan. Masyarakat awam menyebut jenis kartu ini dengan istilah "kartu gesek" atau "swipe card".

Cara kerja teknologi magnetic stripe card pada dasarnya adalah seperti ini: pada saat digesek itulah isi data pita magnetik dibaca, dikirim, diterjemahkan dan diolah pemroses di sisi pusat untuk memeriksa identitas pemegang kartu, validitas dari kartu itu sendiri dan juga keabsahan transaksinya. Proses ini terjadi secara real time dan harus online apabila unit pembaca dan pemrosesnya terpisah.

Kartu magnetik digunakan luas oleh masyarakat untuk berbagai macam keperluan, mulai dari kartu identitas karyawan/mahasiswa/pelajar, SIM hingga kartu akses kamar hotel dlsb. bukan hanya untuk kartu ATM/debit atau kartu kredit. Sehingga perangkat pembaca (reader/skimmer), maupun untuk menulis (recorder) serta aneka software untuk enkripsi/dekripsi data dijual bebas di pasaran. Bukan hal yang luar biasa apabila terjadi penggandaan kartu ATM karena perangkatnya tersedia dan tidak memerlukan keterampilan yang khusus untuk melakukannya. Apalagi teknologi ini sudah digunakan selama sekitar 20 tahun sehingga berbagai macam kelemahan telah diketahui luas dan karenanya sudah sepatutnya mulai digantikan dengan teknologi lainnya yang lebih maju dan aman.

Kartu dengan teknologi baru adalah jenis chip/smart card. Bentuknya seperti yang digunakan pada telepon selular (GSM/CDMA SIM/RUIM card). Ukuran dan formatnya diatur oleh standar internasional (ISO). Chip tersebut bisa berfungsi sebagai memori saja maupun juga sebagai mikroprocessor atau sekaligus keduanya. Pada dasarnya adalah sistem komputer dalam satu chip yang ditanamkan pada kartu plastik. Cara kerjanya dapat melalui kontak langsung dengan cara ditancapkan maupun secara nirkabel, cukup ditempelkan dari jarak dekat pada mesin pembaca atau kombinasi keduanya (hybrid) dan dapat digabungkan dengan teknologi lainnya seperti RFID maupun biometric system.

Biasanya chip card ini juga masih dipasang magnetic stripe untuk kebutuhan backward compatibility (kompatibilitas mundur), terutama untuk aplikasi di sektor perbankan. Karena belum semua jaringan layanan perbankan seperti mesin ATM, EDC telah memiliki kemampuan pembacaan dan pengolahan smart card. Sehingga magnetic stripe tetap dipasang di kartu yang sama sebagai backup.

Kelebihan smart card terutama adalah kemampuan pengolahan transaksi secara offline. Artinya tidak harus terkoneksi real time ke server atau pengolah pusat. Ini dimungkinkan karena seluruh data pada dasarnya telah ditanamkan di dalam chip, bukan hanya identitas tetapi juga termasuk besarnya saldo atau dana yang tersedia. Bahkan dimungkinkan melakukan transaksi langsung dari user ke user tanpa melalui bank. Sehingga kartu jenis ini dapat digunakan untuk beberapa fungsi sekaligus misalnya saja sebagai kartu ATM/debit dan juga sebagai kartu kredit dan voucher sekaligus, jadi praktis.

Smart card juga relatif lebih aman dibanding pendahulunya. Karena memiliki kemampuan processing sendiri selain sebagai memori, maka relatif lebih sulit digandakan dibandingkan jenis kartu magnetic stripe yang bersifat hanya sebagai memori saja. Perlu peralatan khusus untuk mencetak smart card yang harganya jauh lebih mahal dan oleh vendor hanya disediakan dalam jumlah terbatas.

Maka demi keamanan, gunakan hanya kartu chip. Kalau bank belum memberikan kartu chip, Anda harus minta ganti dan jangan menggunakan untuk transaksi sebelum diganti. Aturan Bank Indonesia (BI), sejak Januari 2010 untuk kartu kredit yang boleh digunakan hanya kartu jenis chip.

*) catatan: eksploitasi celah kelemahan smart card juga sudah banyak terjadi dan ada banyak kasus dilaporkan. Misalnya penggandaan chip dan pemindai jarak jauh untuk smart card berbasis teknologi

RFID (kartu voucher yang ditempelkan pada mesin EDC). Sehingga beberapa layanan mulai membuat kombinasi sistem keamanan ganda tidak hanya berbasis PIN dan password melainkan juga biometrik (sidik jari, retina dlsb.). Tapi masalahnya adalah biaya dan kerumitan implementasinya.

3. Perlindungan Kartu Secara Fisik

Kalau kartu anda dapat digunakan pada jaringan internasional, maka biasanya akan memiliki kode 3 angka (CVV2) di belakang kartu Anda. Kecuali untuk otorisasi transaksi online, kode CVV2 tidak akan pernah digunakan. Tutup 3 angka di belakang kartu dengan sticker, cellotape yang tidak transparan. Untuk transaksi konvensional di mesin ATM, counter EDC merchant kode CVV2 juga tidak diperlukan. Apabila kartu rusak, terlipat, patah ataupun hilang, segera lakukan pemblokiran dan minta pengganti. Catat nomor telepon hotline, customer service, fax dan alamat resmi bank penerbit kartu. Gandakan catatan ini pada beberapa tempat yang berbeda namun mudah diakses pada saat genting.

Untuk melindungi kartu jenis RFID (misalnya voucher pra bayar elektronik), saat ini di pasaran banyak dijual casing (seperti jaket/sleeve) anti pemindai. Di kalangan underground banyak dijual peralatan ini (pemindai RFID) dengan harga murah dan bahkan cukup mudah dibuat sendiri (homebrew).

4. Manajemen PIN dan Password

Langkah pengamanan sendiri (self protection) yang perlu dilakukan adalah mengganti PIN ATM, kartu debit/kredit, SMS/mobile banking dan password Internet banking anda sesering mungkin. Parameter sederhana untuk penggantian PIN dan password adalah misalnya ketika anda cukur rambut atau ganti kaos kaki (yang mulai bau), atau ganti sikat gigi (karena sudah mulai kusut) atau tiap kali cek tekanan roda kendaraan, itulah saatnya mengganti PIN. Di stasiun pompa bensin biasanya ada mesin ATM dan anda bisa mengganti PIN ketika sedang melakukan transaksi pembelian BBM.

Selain itu simpanlah PIN di tempat aman dan sandikan catatan itu dengan cara anda sendiri (misalnya dengan menyisipkan angka tambahan), sehingga orang lain tidak mudah menebak PIN anda. Sedangkan untuk password, sebaiknya gunakan kombinasi alfanumerik dan karakter spesial apabila diijinkan oleh sistem. Gunakan frasa panjang (lebih dari 8 karakter) yang tidak mudah dimengerti maknanya secara harfiah. Yang terakhir, jangan pernah memberitahukan PIN dan password kepada siapapun termasuk kepada petugas bank dengan alasan apapun. Karena itu pintu masuk segalanya.

Musuh utama masalah keamanan adalah perilaku (behaviour) manusia itu sendiri, kebiasaan buruk yang diabaikan (permissif). Sebagian besar insiden terjadi akibat eksploitasi kelemahan secara sosial, sehingga tekniknya disebut dengan social engineering (rekayasa sosial). Modus penipuan mengaku undian berhadiah atau petugas bank yang sedang melakukan perawatan atau orang yang mengaku petugas bank dan memberikan bantuan adalah contoh rekayasa sosial tersebut.

*) catatan: manusia punya kelemahan dalam mengingat sejumlah besar PIN dan password, apalagi harus diganti secara periodik. Anda dapat menggunakan software komputer yang disebut password manager untuk mengelola aneka PIN dan password serta perubahannya tanpa harus menghafalkan satu per satu. Software tersebut yang akan melakukan perubahan periodik terhadap password anda bahkan tanpa anda sendiri mengetahui/hapal isi passwordnya. Sehingga teknik social engineering tak akan mudah memperdaya anda. Anda cukup menghafal satu kata kunci pembuka sandi software itu saja. Data hasil penyimpanan disandikan, sehingga walaupun bisa diambil orang lain, tetap saja tidak bisa dibaca secara telanjang. Dengan software ini anda dapat menyimpan dan mengamankan data di tempat yang terpisah untuk memudahkan anda mengaksesnya dan untuk menghindari single point of failure. Misalnya, bila anda hanya menyimpan data PIN dan password di HP atau notebook, maka ada kemungkinan masalah bila justru media itu yang hilang. Dengan software ini anda dapat menyimpan

data di sejumlah tempat dan bisa diakses dari manapun, di Internet misalnya.

5. Tidak Mudah Percaya dan Lakukan Cross Check

Jangan pernah memberikan informasi PIN, password dan data pribadi yang biasa digunakan untuk otorisasi perbankan kepada siapapun dengan alasan apapun termasuk pada customer service bank. Data pribadi seperti misalnya nama gadis ibu kandung dan lainnya, walaupun bukan informasi yang rahasia, namun oleh bank selalu dijadikan kata kunci otentikasi identitas nasabah. Oleh karena itu, sebaiknya informasi tersebut diindungi, tidak mudah diberikan kepada siapapun. Kecuali memang yakin bahwa itu prosedur yang harus dilalui, misalnya ketika melaporkan kehilangan kartu.

Oleh karena itu sangat penting bagi nasabah untuk memahami detail setiap aspek layanan sehingga bisa membedakan manakah prosedur sesungguhnya dan yang ternyata adalah jebakan.

Sekarang banyak sekali pihak ketiga (misalnya perusahaan asuransi) dengan alasan ada kerja sama dengan pihak bank penerbit kartu, menawarkan produknya secara telemarketing dan anda diminta memberikan informasi pribadi tertentu dengan alasan untuk keperluan otentikasi. Resikonya, apabila ternyata bukan telemarketing tetapi dari sindikat pelaku fraud yang mencoba mengorek data dan informasi pribadi, anda tidak pernah tahu dan seolah diposisikan tidak bisa melakukan cross check dalam situasi ini. Lebih bijaksana bersikap tidak mudah percaya dan tetap cross check.

Berhati-hati apabila menerima tawaran dari telemarketing, karena biasanya persetujuan yang anda berikan akan diterjemahkan sebagai kesediaan untuk melakukan auto debet terhadap account anda. Ini berbahaya, lebih baik bila kurang yakin, anda meminta waktu untuk melakukan konfirmasi kepada bank penerbit apakah benar pihak bank punya kerjasama dengan pihak telemarketing tersebut dan bagaimana aturan main serta risikonya. Atau tolak tawaran (telemarketing) itu. Kalau anda tertarik, cukup anda tanyakan kepada petugas telemarketing tsb. nama produk dan siapa penyelenggaranya. Selanjutnya anda sendiri bisa inisiatif yang menghubungi penyelenggara jasa itu dan meminta untuk dilayani. Cara ini lebih aman, lakukan cross check, walau ini perlu partisipasi aktif anda.

Banyak modus kejahatan melakukan eksploitasi psikologis (bagian dari social engineering), seperti di dalam tawaran telemarketing atau undian hadiah. Manusiawi apabila untuk sesaat seseorang akan merasakan euforia ketika diberikan ucapan selamat karena mendapatkan hadiah besar. Tetapi harus tetap waspada dan selalu melakukan cross check walaupun biasanya pelaku akan menekan dengan cara memberikan ancaman halus berupa batas waktu. Sesungguhnya anda tetap punya waktu untuk melakukan cross check. Demikian juga dengan modus penipuan lain, seperti misalnya berita darurat (sanak keluarga memerlukan tindakan medis segera) ataupun perintah misterius dari seseorang yang mengaku sebagai petugas/aparat keamanan. Informasi pribadi milik anda bisa saja digunakan untuk memperdaya orang terdekat anda atau sebaliknya. Siapapun akan mengalami kepanikan apabila ada kabar orang terdekat dalam kondisi kritis, apalagi si pemberi kabar mampu meyakinkan memberikan data-data pribadi yang sangat akurat, sehingga lalai untuk melakukan cross check.

Hal lain yang perlu anda pahami adalah, tidak selalu informasi pribadi itu akan digunakan untuk suatu tujuan jahat seperti penipuan dengan berbagai macam modus yang telah dipaparkan di atas. Di dalam dunia underground economy (pasar gelap di Internet), informasi pribadi seseorang adalah komoditas yang sangat diminati dan dapat diperjualbelikan. Motif yang pertama adalah untuk data marketing. Di dunia nyata, biaya survey market sangatlah mahal dan seringkali harus memberikan kompensasi pada responden. Maka, data informasi profile responden sangatlah berharga. Bila ada yang menjual dengan harga murah, itu bisa menjadi suatu penghematan besar. Motif yang kedua adalah sebagai media bagi jenis kejahatan yang lain, seperti misalnya spammer – perusahaan marketing online yang selalu haus alamat email baru untuk disebarakan unsolicited mail, brosur dan aneka penawaran sampah. Atau pun

digunakan para bot master untuk menyebarkan malware, menginfeksi komputer anda dengan trojan dan menggunakannya sebagai pasukan (bersama ratusan, ribuan komputer lain yang terinfeksi) bots untuk menyerang pihak lain. Di dunia cyber crime, seorang bot master (attacker) bisa disewa untuk melakukan serangan terhadap pihak lain. Dan mereka memanfaatkan komputer anda tanpa disadari. Motif yang ketiga, informasi rahasia anda digunakan untuk tujuan pemalsuan identitas.

Kesimpulannya, jangan mudah percaya dengan permintaan data pribadi. Baik itu melalui permintaan off line, via telepon/telemarketing maupun ketika anda sedang online di Internet. Selalu lakukan cross check dan apabila anda ragu, lebih baik tinggalkan. Keamanan informasi pribadi anda lebih penting dan berharga apabila dibandingkan aneka tawaran yang mungkin diberikan kepada anda.

*) catatan: bank menerapkan suatu teknik pengamanan yang disebut dengan psuedo security, yaitu serangkaian prosedur yang seolah merupakan pengamanan padahal sebenarnya bukan. Prosedur itu diadakan untuk menciptakan rasa aman semu bagi awam, baik itu nasabah maupun manajemen bank itu sendiri. Misalnya, informasi pribadi yang seolah adalah rahasia dan karenanya dijadikan basis data untuk otorisasi seperti nama gadis ibu kandung. Pada prinsipnya nama gadis ibu kandung bukanlah informasi yang rahasia, karena tentu saja banyak orang yang telah mengetahuinya. Sehingga kalau ada yang berniat jahat, bisa saja mengumpulkan informasi tersebut dan merangkainya sedemikian rupa untuk digunakan mengelabui customer service bank (misalnya via phone banking). Kelemahan psuedo security inilah yang dimanfaatkan oleh para pelaku kejahatan fraud, misalnya dengan kedok undian hadiah atau mengaku sebagai customer service bank, mitra asuransi dlsb. Istilah lain yang mirip dan sangat dikenal di dalam dunia keamanan informasi adalah prinsip security through obscurity. Alasan bank menerapkan pengamanan semu adalah justru demi untuk kenyamanan nasabah, sebab bila sistem pengamanan yang sesungguhnya diterapkan maka akan menyulitkan. Bila pengamanan makin ketat maka tingkat kenyamanan dan kemudahan layanan akan semakin menurun.

6. Berhati-hati Saat Bertransaksi

Modus kejahatan skimming sebenarnya tidak hanya dilakukan di mesin ATM, namun juga terjadi pada transaksi di mesin EDC counter merchant. Bahkan modus ini relatif lebih mudah dilakukan pelaku bila dibandingkan dengan ATM skimmer karena tidak diperlukan kamera pengintip. Beberapa kasus sudah pernah terbongkar sebelumnya. Pilih merchant yang anda yakini benar reputasinya.

Awasi terus keberadaan kartu anda ketika berada di counter merchant, jangan biarkan kartu dibawa kemana-mana dan digesek ke mesin EDC yang berbeda berkali-kali. Lebih baik anda membatalkan transaksi, tidak usah menandatangani apapun dan laporkan ke bank penerbit apabila curiga dengan kondisi di suatu counter merchant. Kalau memungkinkan periksa kondisi mesin EDC, apakah nampak ada perangkat tambahan atau sambungan kabel tambahan yang mencurigakan. Tapi ini perlu sedikit pemahaman teknis, pengguna awam tentu akan sulit membedakan. Namun aksi anda yang seolah tahu kondisi mesin EDC itu mungkin bisa mencegah pelaku dan mengurungkan niatnya.

Patut untuk diingat, begitu kartu digesekkan ke mesin EDC, maka semua informasi penting di dalam magnetic stripe akan tercatat oleh mesin EDC dan sebagian bahkan akan di print out. Seperti nama, nomor kartu dan tanggal masa berlaku (kadang kala tanggal mulai menggunakan). Seseorang tidak perlu punya ingatan super untuk menghafal deretan kode angka yang tertera di kartu. Kalau anda lengah cukup banyak waktu bisa digunakan pelaku untuk mencatat informasi itu atau dengan teknik sederhana menggosok deretan angka yang menonjol (embossed) pada kartu dengan kepingan uang logam pada kertas karbon nota pembelian yang selalu tersedia di meja kasir (thrasing). Bahkan mereka bisa saling kerja sama misalnya berdua, satu orang sengaja mengalihkan perhatian anda dan satunya yang membawa kartu mencatat atau bahkan menggesekkan kartu anda ke mesin skimming yang tidak terlihat. Maka sebaiknya anda berusaha terus mengawasi transaksi tersebut.

Selalu berhati-hati dan harus melakukan pemeriksaan berulang terhadap transaksi dan mencari tahu terlebih dahulu kredibilitas merchant, ketika anda memutuskan untuk melakukan transaksi online di Internet. Perhatikan pula produk yang dijual, apakah benar memiliki kualitas seperti yang dijanjikan ataukah hanya tipuan? Sebaiknya hanya lakukan transaksi di situs yang sudah terkenal dan diketahui reputasinya. Selain lebih meyakinkan, kualitas barang yang ditawarkan pun sesuai.

Banyak sekali situs transaksi online yang tidak kredibel, untuk menjebak konsumen dan mendapatkan informasi kartu kreditnya. Situs transaksi online yang kredibel biasanya memiliki referensi dari pihak ketiga, ada jaminan transaksi pada pelanggan (seperti asuransi, sistem tracking pengiriman barang, garansi). Periksa semua referensi, apakah benar ada atau ternyata hanya tipuan. Lakukan pencarian dengan search engine apakah ditemukan keluhan mengenai situs transaksi tersebut.

Selalu gunakan kartu kredit atau kartu debit yang paling rendah limitnya ketika melakukan transaksi online, untukantisipasi seandainya terjadi fraud. Atau yang lebih bijaksana, gunakan layanan online payment (e-money) pihak ketiga seperti paypal untuk menghindari transaksi langsung menggunakan kartu kredit. Anda dapat mengisikan dana dari kartu kredit ke layanan uang elektronik dalam jumlah yang terbatas sehingga aman dari upaya pembobolan. Selanjutnya untuk transaksi dengan merchant online dilakukan dengan pembayaran melalui e-money ini. Merchant yang bisa menerima pembayaran dengan e-money punya kredibilitas yang meyakinkan karena dipercaya provider e-money.

Namun bila tetap tidak yakin dengan keamanan kartu kredit dan informasi pribadi anda, sebenarnya masih ada alternatif lain untuk transaksi online, yaitu dengan menggunakan metode pembayaran wire transfer. Cara ini lebih meyakinkan walaupun lebih lama prosesnya dan anda harus menyediakan uang tunai serta tidak bisa menikmati manfaat pembayaran tunda serta fasilitas cicilan tetap yang banyak ditawarkan oleh kartu kredit. Wire transfer juga bisa digunakan untuk mengisi e-money.

*) catatan: perlu diketahui, tidak semua mesin EDC di counter merchant berasal dari bank, atau tidak dalam pengendalian dan pengawasan bank sepenuhnya. Mesin EDC itu mungkin saja disediakan oleh pihak ketiga (vendor outsourcing, perusahaan payment gateway dlsb. Bahkan seperti mesin ATM ada pula yang menyewakan). Akibatnya sangat mungkin terjadi penyimpangan mesin EDC.

7. Sadar Lingkungan Transaksi

Ketika anda akan bertransaksi di mesin ATM, hal pertama yang harus anda lakukan adalah mencari mesin ATM yang sekiranya aman. Pilihlah mesin ATM yang berada di tempat terbuka dan selalu ramai dikunjungi dan selalu diawasi keamanannya, misalnya di pusat perbelanjaan. Hindari mesin ATM yang berada di lokasi yang terpencil, gelap, sepi dan tanpa penjagaan atau pengawasan.

Kalau anda sedang terburu-buru, tidak sempat memeriksa kondisi mesin ATM maka langkah paling aman adalah menggunakan outlet yang ada di bank itu sendiri. Setiap kantor cabang, biasanya kini telah menyediakan mesin ATM yang relatif terjaga kondisinya karena ada petugas keamanan 24 jam (walaupun perlu dipahami bahwa tugas petugas keamanan sebenarnya bukan mengamankan mesin ATM, melainkan menjaga kantor cabang – mesin ATM termasuk properti kantor tsb.).

Periksalah kondisi mesin ATM. Perhatikan mulut lubang card reader, apakah ada bekas lem, tempelan atau benda lain yang mencurigakan (karena tidak seharusnya berada di situ). Untuk memastikannya, goyangkan sedikit apabila ada benda asing di sekitar mesin ATM (misalnya kotak pengumuman yang ada di samping mesin ATM), celah di sekitar mesin atau di atap, untuk memeriksa apakah tidak ada peralatan tersembunyi di dalamnya, misalnya kamera. Pastikan mulut lubang card reader ATM telah dilindungi dengan tutup anti skimmer. Cermati apa papan tombol numerik (keyboard) telah dilindungi

dengan penutup. Bila tidak yakin, ketika memasukkan PIN, lindungi dan tutupi tangan anda sehingga sulit diintip. Periksa pula apa tidak ada benda lain yang menutupi keyboard, karena pelaku skimmer bisa saja memasang bantalan tambahan yang menyerupai keyboard dan berfungsi sebagai keylogger (perekam keyboard). Bila anda tidak yakin dengan prosedur ini, setiap saat anda bisa meninggalkan mesin ATM tersebut dan mencari lokasi lain yang lebih terjamin keamanannya.

Jangan pernah percaya dengan tawaran bantuan dari orang di sekitar mesin ATM termasuk itu yang mengaku sebagai satpam atau petugas bank. Apabila anda mengalami kesulitan, lebih baik telepon customer service bank dan biarlah masalah anda diatasi oleh mereka – itu sebabnya mengapa anda harus memiliki catatan nomor kontak resmi bank. Jangan pernah percaya informasi dari orang lain di sekitar mesin ATM atau stiker yang seolah menunjukkan nomor kontak resmi bank, karena bisa saja ternyata bukan dan ini adalah jebakan pelaku fraud. Bila kartu anda tersangkut di mesin ATM, maka tinggalkan saja tanpa melakukan apapun kecuali langsung menghubungi CS bank segera diblokir dan meminta kartu baru. Ingat, dalam prosedur pelaporan ini anda tidak akan diminta menyebutkan nomor PIN. Bila CS atau yang mengaku CS bank menanyakan PIN, tutup saja teleponnya.

Jika anda merasa mengalami penipuan ataupun kejanggalan, lebih baik laporkan kepada bank atau apabila anda telah menderita suatu kerugian, laporkan kepada kepolisian terdekat.

Kewaspadaan yang sama harus anda terapkan ketika menggunakan Internet banking. Syarat utama yang harus dipenuhi adalah memastikan bahwa terminal akses yang anda gunakan aman. Gunakan selalu terminal akses milik anda sendiri (misalnya laptop) yang anda yakini kemanannya. Bila anda menggunakan terminal akses publik (misalnya di warnet, di kampus, di kantor) atau milik orang lain maka pastikan bahwa terminal tersebut bersih dari virus, trojan dan aplikasi berbahaya seperti key logger. Anda harus melakukan hard booting terlebih dahulu sebelum bertransaksi untuk menghapus sejumlah program jahat yang mungkin residen di memori (misalnya key logger) dan melakukan scan menyeluruh dengan anti virus serta anti malware terbaru (sejumlah aplikasi tools pemeriksa ini bisa anda pasang di sebuah media penyimpan USB portabel). Proses ini perlu waktu.

Anda juga harus membiasakan akses dengan menggunakan browser yang aman atau menggunakan aplikasi browser portabel milik anda sendiri. Beberapa layanan Internet banking sudah menyediakan keyboard virtual pada halaman web sehingga anda tidak perlu memasukkan satu huruf atau angka pun dari keyboard komputer. Cara ini lebih aman, namun ternyata belum semua bank menerapkan. Anda juga harus dapat mengenali model penipuan menggunakan teknik phishing dan bagaimana cara menghindarinya serta disiplin untuk tidak mengaktifkan opsi fitur otomatis merekam username dan password. Setiap kali selesai melakukan transaksi, hapus pula cookies dan cache.

Tidak cukup sampai di situ, anda juga harus memastikan keamanan saluran akses yang digunakan. Bertransaksi Internet banking menggunakan layanan WiFi (wireless) di sebuah cafe adalah contoh yang sangat tidak dianjurkan. Karena layanan WiFi sangat rawan penyadapan dan teknik ini terlalu mudah untuk dilakukan. Bisa jadi seorang pengguna laptop yang ada di seberang meja anda itulah attacker yang sedang menyadap semua informasi penting dari laptop anda dan mencatat transaksi Internet banking anda termasuk username, password bahkan algoritma token bank.

Perlu anda ketahui, walaupun sudah menggunakan pengaman token, namun bukan berarti algoritma kunci dari tools ini tidak dapat didekripsi oleh pelaku kejahatan. Dengan teknik tertentu token dapat dibobol dan diduplikasi dengan menggunakan software tools pembongkar algoritma.

Menggunakan terminal yang bersih dan diyakini keamanannya serta saluran fixed (kabel) private saat melakukan transaksi melalui Internet banking adalah pilihan yang paling bijaksana.

Terakhir, menggunakan layanan SMS/mobile banking adalah jenis transaksi yang paling tidak aman karena hanya mengandalkan otentikasi berdasarkan nomor HP dan PIN. Tidak ada cara pengamanan tambahan misalnya koneksi yang terenkripsi, metode otentikasi tambahan dan pemakaian token atau one time access code. Anda perlu mengetahui bahwa nomor HP (di Indonesia hampir semua operator menggunakan SIM/RUIM card) dapat dengan mudah digandakan (cloning). Sedang PIN dapat dengan diperoleh misalnya melalui social engineering. Maka, bila anda masih bisa melakukan transaksi dengan cara lain, tidak selalu dalam kondisi mobile, tidak harus melakukan transaksi segera, gunakanlah cara lain, hindari menggunakan fasilitas dan fitur serta layanan SMS/mobile banking. Bahkan mungkin saja anda tidak perlu mengaktifkan layanan ini apabila memang tidak memerlukannya.

Ketika anda secara intensif memanfaatkan teknologi untuk memfasilitasi dan mempermudah aktivitas kehidupan sehari-hari, maka sadarilah bahwa anda juga harus memahami resiko yang menyertai dan memahami bagaimana cara meminimalisir dampak yang mungkin terjadi. Perilaku waspada dan sadar resiko itu menjadi tanggung jawab dan peran anda dalam upaya pengamanan. Karena, *your security is my security*. Bukan hanya menjadi urusan bank, pemerintah dan penyedia layanan.

Pihak Bank Indonesia, industri perbankan, aparat keamanan dan pemerintah mempunyai kewajiban dan tanggung jawab kepada masyarakat untuk secara berkelanjutan memberikan edukasi mengenai jenis layanan yang memanfaatkan teknologi, karakteristik, aturan main dan resiko yang mungkin saja terjadi. Kampanye semacam ini dapat mematikan niat dan modus pelaku kejahatan.

(Indonesia Security Incident Response Team on Internet Infrastructure – ID-SIRTII)