Kenapa Perbankan Internet? tidak perlu beratur untuk urusan urusan perbankan 24 jam berurusan dari rumah, luar negara, tepi pantai dan di mana saja caj yang lebih murah Perbankan Internet membolehkan anda menguruskan hal ehwal kewangan anda dari rumah, tempat kerja atau di mana-mana sahaja di serata dunia.Pada masa ini, hanya institusi-institusi perbankan yang berlesen sahaja yang dibenarkan untuk menawarkan perkhidmatan perbankan Internet di Malaysia. Senarai institusi-institusi perbankan berlesen yang telah diluluskan oleh Bank Negara Malaysia untuk menawarkan perkhidmatan perbankan Internet boleh diperolehi di laman sesawang Bank Negara Malaysia, www.bnm.gov.my. PERKHIDMATAN PERBANKAN YANG DITAWARKAN DALAM TALIAN Bergantung kepada institusi perbankan, perkhidmatan utama yang ditawarkan melalui perbankan Internet membolehkan anda: <ul> Menyemak baki akaun dan penyata akaun Mengemukakan permohonan untuk akaun, kad kredit atau kemudahan pinjaman baru Membuat pelaburan deposit tetap Memindah dana di antara akaun (milik sendiri dan pihak ketiga) Memindah dana ke dalam akaun ASB (Amanah Saham Bumiputera) Membayar bil, kad kredit, pinjaman, premium insurans dan perkhidmatan yang ditawarkan oleh badan kerajaan/swasta Membuat, meminda dan membatalkan arahan tetap Memohon buku cek dan penyata akaun Menyemak status cek dan memohon arahan menghentikan pembayaran cek Memohon draf bank dan pemindahan telegraf Membeli kredit pra-bayar telefon bimbit SEBELUM ANDA MENDAFTAR Anda dinasihatkan supaya membaca dan memahami terma dan syarat-syarat perkhidmatan sebelum mendaftar untuk menggunakan perkhidmatan perbankan Internet. Anda juga harus berbincang dengan institusi perbankan anda mengenai risiko yang berkaitan dengan perbankan Internet dan memahami tanggungjawab serta hak-hak anda sepenuhnya. ADAKAH PERKHIDMATAN PERBANKAN INTERNET SELAMAT DIGUNAKAN? Seperti sistem-sistem lain, penggunaan perbankan Internet turut mengandungi risiko. Walau bagaimanapun, tahap risiko telah diminimumkan melalui pemeriksaan sistem keselamatan secara berterusan oleh institusi perbankan dan sikap berhati-hati anda apabila menggunakan perkhidmatan perbankan Internet. Tindakan institusi perbankan untuk menjamin keselamatan <ul> Institusi perbankan dikehendaki memastikan sistem perbankan Internet selamat digunakan oleh pengguna. Tambahan pula, institusi perbankan yang menawarkan perbankan Internet juga dikehendaki mematuhi garis panduan minimum yang ditetapkan oleh Bank Negara Malaysia. Tindakan yang patut anda lakukan untuk menjamin keselamatan perbankan Internet ID log masuk dan kata laluan atau nombor PIN <ul> Lakukan <ul> Hafal dan jangan menulisnya di mana-mana Sentiasa menukar kata laluan atau nombor PIN Gunakan kata laluan yang mempunyai kombinasi huruf kecil, huruf besar dan nombor. Berhati-hati menggunakan pautan di e-mel, &#65533;instant message&#65533;, atau &#65533;chat&#65533; untuk ke laman sesawang bank jika anda mencurigai kesahihan atau tidak mengenali pengirim mesej tersebut. Berusaha untuk menelefon pihak bank atau menaip alamat laman sesawang bank terbabit di pelayar sesawang. Berhati-hati dengan panggilan telefon daripada penjenayah yang mungkin juga kelihatan seperti panggilan rasmi daripada pihak bank kerana penjenayah menyalahguna teknologi &#65533;Voice Over IP&#65533; untuk mengelirukan pengguna bagi mendapatkan maklumat sulit. Tukar kata laluan atau nombor PIN anda dengan serta-merta dan menghubungi institusi perbankan anda jika anda mengesyaki adanya transaksi yang tidak

dibenarkan ke atas akaun anda atau terdapat pihak lain yang mungkin mengetahui kata laluan atau nombor PIN anda. Sentiasa menyemak butir-butir sejarah transaksi dan penyata anda untuk memastikan tiada transaksi yang tidak dibenarkan dan tiada tambahan kepada senarai penerima bayaran yang berdaftar.   Jangan <ul> Hantar maklumat peribadi anda terutamanya kata laluan atau nombor PIN melalui e-mel biasa, sistem pesanan ringkas (SMS), &#65533;pop-up message&#65533; mahupun melalui mana-mana aplikasi &#65533;Instant Messages&#65533; (e.g.Yahoo Messenger, Facebook). Menyimpan ID log masuk dan kata laluan atau nombor PIN anda dalam komputer ataupun telefon bimbit. Mengguna kata laluan yang mudah diteka seperti nama atau tarikh lahir. Melayan sebarang permintaan untuk mendapatkan ID log masuk dan kata laluan, nombor PIN atau butiran akaun perbankan anda melalui telefon, faks, e-mel ataupun SMS, walaupun ia kelihatan seperti urusan rasmi atau penting kerana institusi perbankan tidak akan meminta maklumat perbankan daripada pelanggan melalui cara tersebut.   Pastikan bahawa anda berada di laman sesawang yang betul dan selamat <ol> Sentiasa memasukkan "Uniform Resource Locator&#65533; (URL) laman sesawang secara terus pada pelayar sesawang. Elakkan daripada masuk ke laman sesawang bank atau hiperpautan ke laman sesawang tersebut daripada e-mel atau laman sesawang yang lain. Pastikan anda berada di laman sesawang yang betul sebelum mengendalikan transaksi dalam talian atau menghantar maklumat peribadi Pastikan anda berada di laman sesawang yang selamat dengan menyemak URL yang dimulai dengan &#65533;https://&#65533; dan bukannya &#65533;http://&#65533; serta pastikan simbol mangga berkunci (&#65533;padlock&#65533;) seperti gambar rajah di bawah tertera pada bar status pelayar sesawang anda. Walau bagaimanapun, anda haruslah berwaspada tentang kemungkinan URL dan imej ibu kunci tertutup yang mewakili sijil &#65533;Secured Socket Layer&#65533; (SSL) adalah palsu. Oleh itu, periksa URL dan sijil SSL daripada tab &#65533;Page Properties&#65533; untuk mengenal pasti kesahihan laman sesawang tersebut. Pasang &#65533;toolbar&#65533; pelayar sesawang yang dapat memberi amaran tentang laman sesawang &#65533;phishing&#65533; agar risiko anda terjebak ke dalam penipuan &#65533;phishing&#65533; dapat dikurangkan. Tindakan yang patut anda lakukan untuk menjamin keselamatan perbankan Internet <ul> Mendaftar untuk menggunakan kaedah pengesahan yang lebih baik <ul> Daftar untuk menggunakan kaedah pengesahan pelbagai faktor, iaitu pengesahan pelbagai peringkat akan dilakukan untuk melindungi transaksi anda. Sesetengah institusi perbankan menggunakan TAC (Transaction Authorisation Code) yang dihantar ke nombor telefon mudah alih pengguna atau alat &#65533;token&#65533; yang memaparkan kod khas dan perlu dimasukkan pengguna dalam perbankan Internet sebelum melakukan transaksi berisiko tinggi.   Lindungi komputer peribadi anda daripada penceroboh, virus dan program perosak <ul> Pasang dinding keselamatan (&#65533;firewall&#65533;) peribadi dan program penentang virus yang baik untuk mengelakkan komputer peribadi anda daripada diserang oleh virus, pengintip dan program perosak seperti "Trojan Horse" Pastikan program penentang virus dan penentang pengintip anda adalah yang terkini dan sentiasa dikemas kini. Pastikan sistem kendalian dan pelayar sesawang anda adalah yang terkini dan dilengkapi dengan ciri-ciri keselamatan yang terbaru untuk melindunginya daripada dieksploitasi. Jadikan pelayar anda berupaya untuk menolak kawalan ActiveX bagi mengurangkan kebarangkalian aplikasi pengintip dipasang ke dalam komputer anda   Berhati-hati apabila memuat turun perisian <ul> Periksa program atau lampiran yang diterima dengan program penentang virus yang terkini untuk memastikan ia tidak mengandungi virus yang boleh

menyerang komputer anda Jangan sesekali memuat turun sebarang fail atau perisian daripada laman web atau sumber yang kurang anda kenali atau klik pada hiperpautan yang dihantar oleh seseorang yang tidak anda ketahui. Pembukaan fail, perisian atau hiperpautan sedemikian boleh mendedahkan sistem anda kepada virus komputer yang boleh mencuri maklumat peribadi anda, termasuk kata laluan atau nombor PIN anda   Sentiasa ingat untuk log keluar <ul> Apabila selesai melaksanakan transaksi perbankan Internet, anda hendaklah terus log keluar. Padamkan peti ingatan dan sejarah transaksi selepas log keluar untuk menghapuskan sebarang maklumat tentang akaun anda. Ini adalah penting untuk mengelakkan maklumat yang tersimpan daripada diambil oleh pihak yang tidak bertanggungjawab. Elakkan meninggalkan komputer yang masih beroperasi tanpa pengawasan.   Langkah-langkah lain <ul> Jangan biarkan tetingkap pelayar yang lain dalam keadaan terbuka semasa membuat transaksi perbankan dalam talian. Elakkan mengguna komputer yang dikongsi bersama atau milik awam seperti di kafe Internet untuk mengendalikan transaksi perbankan Internet anda. Elakkan melakukan transaksi perbankan internet melalui rangkaian bebas wayar awam percuma (�free public wi-fi/hotspots�) walaupun anda menggunakan komputer peribadi sendiri. Mengenyahaktifkan ciri-ciri perkongsian fail, fungsi �auto complete� di pelayar sesawang dan mesin pencetak dalam sistem kendalian anda. Jika anda mempunyai sebarang persoalan tentang keselamatan akaun Internet anda, hubungilah institusi perbankan anda untuk membincangkan isu tersebut, termasuk cara penyelesaiannya.   ANCAMAN KESELAMATAN INTERNET !!! �Pharming� - Tindakan mengeksploitasi kelemahan perisian sistem nama domain (DNS) yang membolehkan penceroboh mendapatkan nama domain institusi perbankan yang sebenar dan menukar arah laluan trafik daripada laman sesawang institusi perbankan tersebut ke laman sesawang palsu. �man-in-the-middle� - Serangan yang dapat membaca, menambah dan mengubah mesej di antara anda dan institusi perbankan anda tanpa kedua-dua pihak mengetahui bahawa pautan tersebut telah diceroboh. �Phishing� - Merupakan tindakan menghantar e-mel atau SMS palsu kepada mangsa <ul> SMS Scam - Penjenayah akan menghantar SMS yang menawarkan hadiah lumayan kononnya daripada syarikat-syarikat terkemuka untuk menarik mangsa. Bagi mendapatkan hadiah tersebut, mangsa harus akur dengan prosedur yang ditetapkan penjenayah, iaitu mangsa harus ke mesin ATM untuk mendaftar akaun perbankan Internet (sekiranya mangsa belum mempunyai akaun perbankan Internet) disertai nombor telefon bimbit penjenayah sebagai nombor rasmi untuk urusan perbankan (bagi tujuan penerimaan TAC). Setelah itu, maklumat sulit seperti nombor PIN akan diberikan kepada penjenayah. Penjenayah akan mendaftar untuk urusan perbankan internet bagi pihak mangsa dan melakukan pindahan dana ke akaun penjenayah. Kepada mangsa yang sudah mempunyai akaun perbankan internet, mereka hanya perlu mendedahkan ID dan kata laluan perbankan Internet mereka kepada penjenayah. Penjenayah seterusnya menggunakan maklumat sulit tersebut untuk mengakses akaun perbankan Internet mangsa. �Phishing site� - E-mel palsu yang didakwa dihantar oleh institusi perbankan akan mengumpan penerima untuk mengemas kini profil perbankan Internet mereka dengan cara mengklik pautan laman perbankan Internet palsu dan memasukkan maklumat peribadi mereka di dalam �phishing site� tersebut. Pengguna lazimnya tertipu kerana laman sesawang �phishing� mengandungi logo, format, grafik dan perkataan-perkataan yang seakan-akan laman perbankan Internet sebenar. Penjenayah akan menggunakan maklumat perbankan Internet yang dicuri daripada laman sesawang �phishing�

berkenaan untuk mengakses akaun perbankan mangsa dan memindahkan wang mangsa ke akaun pihak ketiga.   KERAHSIAAN MAKLUMAT PERIBADI ANDA Institusi perbankan dan anda mempunyai peranan dalam memastikan kerahsiaan terjamin. Keselamatan maklumat peribadi dan kewangan anda adalah perkara yang amat penting apabila mengendalikan transaksi perbankan melalui Internet. Kerahsiaan maklumat peribadi pengguna adalah satu unsur penting kepercayaan dan keyakinan orang ramai terhadap sistem perbankan. Pengguna boleh menghubungi Cyber999 (MyCERT-Malaysia Computer Emergency Response Team) melalui talian rasmi ataupun SMS untuk melaporkan ancaman keselamatan internet: Talian Rasmi Cyber9999:00 AM 6:00 PM : 1-300-88-299924x7 (Kecemasan): +6019 - 266 5850Sistem Pesanan Ringkas (SMS)Format SMS untuk di hantar ke 15888:CYBER999 REPORT to 15888Sumber: Bank Negara Malaysia