Dasar Keselamatan

Untuk Perkhidmatan Perbankan Digital Hong Leong Bank Connect

Semua data peribadi yang anda berikan kepada HLBB/HLISB atau yang diperoleh HLBB/HLISB daripada domain awam, serta data peribadi yang diperoleh daripada peruntukan Perkhidmatan HLBB/HLISB kepada anda, sama ada melalui Hong Leong Bank Connect atau sebaliknya, adalah tertakluk kepada Dasar Privasi HLBB/HLISB yang boleh dipinda dari semasa ke semasa. Salinan Dasar Privasi HLBB/HLISB disediakan apabila diminta atau boleh didapati di laman web HLBB/HLISB.

Langkah Keselamatan yang Diambil untuk Melindungi Maklumat

Kami melindungi maklumat anda dengan selamat di pusat data keselamatan tinggi yang mematuhi kawalan, langkah dan protokol keselamatan yang ketat bagi menjamin privasi maklumat anda. Walaupun kami akan berusaha sedaya upaya untuk memastikan privasi semua Maklumat disimpan selamat, sila ambil perhatian bahawa secara umumnya diketahui bahawa penghantaran data melalui Internet dan/atau saluran elektronik lain tidak dijamin selamat sepenuhnya. Oleh yang demikian, sila pastikan maklumat anda tidak boleh diakses atau didedahkan kepada sesiapa. Seterusnya kami juga tidak bertanggungjawab dan tidak menanggung liabiliti atas sebarang kerosakan atau kerugian yang mungkin anda alami, sama ada secara langsung atau tidak langsung, akibat Maklumat tersebut dicuri, diganggu, disalin, disalahgunakan, disalah pakai atau sebaliknya dicabuli. Untuk maklumat lanjut tentang langkah keselamatan kami, sila rujuk Kenyataan Keselamatan kami di bawah.

Kenyataan Keselamatan

Kami di Hong Leong Bank Berhad ("HLBB") dan Hong Leong Islamic Bank ("HLISB") akan sepanjang masa berusaha memastikan bahawa semua maklumat yang didedahkan, dikongsi, disimpan atau digunakan dan sebarang transaksi yang dilaksanakan oleh anda melalui laman web perbankan digital Hong Leong Bank Connect ("HLB Connect") adalah lancar, selamat, peribadi dan rahsia. Untuk itu, kami telah melaksanakan langkah keselamatan dan sistem kawalan perlindungan privasi yang direka untuk memastikan keselamatan, integriti, privasi dan kerahsiaan maklumat dan transaksi anda tidak terjejas.

Nama Pengguna dan Kata Laluan

Untuk mengawal akses perkhidmatan perbankan digital HLB Connect kami, setiap pelanggan perlu memasukkan nama pengguna dan kata laluan mereka. Nama pengguna dan kata laluan ini adalah kunci akses kepada maklumat kewangan anda. Untuk memastikan integriti kata laluan, anda dinasihatkan untuk melakukan langkah berikut:-

- Semasa memilih kata laluan, jangan pilih kata laluan yang mudah diteka oleh orang lain.
- Elak daripada menggunakan maklumat peribadi seperti nama anda , tarikh lahir, nombor telefon atau perkataan yang tersenarai dalam kamus standard.
- Ingat kata laluan anda dan jangan tulis kata laluan anda.
- Kata laluan tidak boleh sama sekali didedahkan atau diakses oleh sesiapa. Kata laluan tidak boleh didedahkan walaupun diminta untuk berbuat demikian oleh pegawai HLBB/HLISB yang sah.

- Untuk perlindungan tambahan, anda digalakkan mengubah kata laluan anda dari semasa ke semasa.
- Jika anda terlupa kata laluan, anda boleh set semula HLB Connect anda.

PIN ATM

Pelanggan yang menggunakan mod ATM atau Kad Debit pendaftaran kali pertama atau set semula HLB Connect perlu memasukkan PIN ATM mereka. PIN ATM 6 digit ini bersama dengan Nombor ATM/Kad Debit anda yang aktif serta Nombor Kad Pengenalan/Pasport membolehkan anda mendaftar atau set semula HLB Connect bagi mencipta atau menukar Nama Pengguna dan Kata Laluan anda.

PIN Kad

Pelanggan yang menggunakan mod Kad Kredit pendaftaran kali pertama atau set semula HLB Connect perlu memasukkan PIN Kad mereka. PIN Kad 6 digit ini bersama dengan Nombor Kad Kredit anda yang aktif dan Nombor Kad Pengenalan/Pasport membolehkan anda mendaftar atau set semula HLB Connect bagi mencipta atau menukar Nama Pengguna dan Kata Laluan anda.

ID Sementara

Pelanggan yang menggunakan mod Nombor Akaun pendaftaran kali pertama atau set semula HLB Connect perlu memasukkan ID Sementara mereka. ID 10 aksara yang terdiri daripada huruf dan nombor ini bersama dengan Nombor Akaun anda yang sah serta Nombor Kad Pengenalan/Pasport membolehkan anda mendaftar atau set semula HLB Connect bagi mencipta atau menukar Nama Pengguna dan Kata Laluan anda.

- ID Sementara boleh diminta melalui mana-mana cawangan HLBB/HLISB.
- ID Sementara sah selama tiga (3) hari dan hanya boleh digunakan sekali sahaja.

Kod Pengesahan Transaksi

Bagi sesetengah transaksi kewangan, pelanggan perlu meminta dan memasukkan Kod Pengesahan Transaksi ("TAC") bagi mengesahkan transaksi. TAC akan diberikan secara automatik melalui dalam talian apabila anda melaksanakan pendaftaran kali pertama atau set semula HLB Connect anda atau menjalankan transaksi kewangan yang tertentu. Setiap TAC hanya sah untuk satu transaksi sahaja dan akan tamat selepas 3 minit. TAC tidak boleh sama sekali didedahkan atau diakses oleh sesiapa. TAC tidak boleh didedahkan walaupun diminta untuk berbuat demikian oleh pegawai HLBB/HLISB yang sah.

Privasi Data, Kerahsiaan dan Integriti

Bagi memastikan privasi data, kerahsiaan dan integriti, semua maklumat yang didedahkan, dikongsi, disimpan atau digunakan dan sebarang transaksi yang dilaksanakan oleh anda melalui laman web perbankan digital HLB Connect dienkripsikan menggunakan "256-bit Secure Sockets Layer" daripada Pihak Berkuasa Pensijilan Verisign.

Keselamatan Sistem dan Pengawasan

Bagi menyediakan persekitaran yang selamat untuk laman web HLB Connect, HLBB/HLISB menggunakan gabungan langkah keselamatan sistem dan pengawasan:

- Sistem dinding api, enkripsi data yang kukuh, perlindungan anti virus dan sistem pengawasan keselamatan sepanjang masa untuk mengesan dan mencegah sebarang bentuk aktiviti haram dalam sistem rangkaian kami.
- Penggunaan gambar keselamatan tambahan untuk mengesahkan akses ke laman web perbankan digital HLB Connect dan identiti pelanggan yang betul.
- Log keluar HLB Connect secara automatik apabila tiada aktiviti dikesan untuk tempoh masa tertentu.
- Tidak membenarkan akses ke HLB Connect selepas tiada aktiviti selama 3 bulan.
- Semakan keselamatan yang kerap dijalankan terhadap sistem oleh Juruaudit Sistem dalaman kami serta pakar keselamatan luaran.
- Kerjasama dengan vendor/pembuat utama untuk mendapat maklumat perkembangan teknologi keselamatan dan melaksanakan apa yang relevan.

Tanggungjawab Pelanggan

Kami di HLBB/HLISB sentiasa mengemaskinikan teknologi keselamatan untuk melindungi privasi dan kerahsiaan anda, tetapi kami tiada kawalan terhadap peranti elektronik yang anda gunakan untuk mengakses HLB Connect atau telefon mobile yang anda gunakan untuk menerima TAC atau kod keselamatan lain yang serupa, yang mungkin dikeluarkan oleh HLBB/HLISB dari semasa ke semasa.

Sila berhati-hati dan sentiasa berjaga-jaga terhadap e-mel yang mencurigakan atau panggilan telefon/SMS yang meminta maklumat peribadi atau berkaitan akaun perbankan anda yang bertujuan melakukan pencurian dan penipuan internet. Jangan balas mana-mana e-mel atau SMS dengan pautan URL internet yang memerlukan anda memasukkan data kelulusan keselamatan dalam talian seperti nama pengguna, kata laluan dan TAC.

Anda bertanggungjawab menjaga maklumat dan transaksi dalam talian dengan mengambil semua langkah yang wajar termasuklah yang berikut:

- Jangan berkongsi maklumat anda atau memberi peluang kepada sesiapa daripada mendapat akses kepada maklumat anda melalui peranti elektronik peribadi anda.
- Sentiasa log masuk URL yang betul (www.hongleongconnect.my) dan anda dapat lihat gambar keselamatan yang betul semasa memasukkan Nama Pengguna anda.

- Sentiasa log keluar sebelum melawat laman Internet lain atau selepas menyelesaikan transaksi anda.
- Sentiasa pastikan anda memiliki perisian keselamatan dan dinding api yang dikehendaki dan sesuai dipasang pada komputer anda, terutamanya jika anda menggunakan sambungan internet tanpa wayar.
- Sentiasa kemas kini pelayar internet anda apabila versi baharu diperkenalkan kerana selalunya versi ini memiliki ciri keselamatan terkini.
- Periksa pelayar internet anda untuk ciri keselamatan binaan dalam yang anda mungkin atau tidak mungkin pilih untuk digunakan.
- Periksa sijil laman web sebelum log masuk.
- Sentiasa bersihkan cache internet selepas anda log keluar daripada sesi dalam talian.