Tingkatkan keamanan rekening Anda dengan langkah bijak

Perhatikan keamanan halaman website Anda

Saat login ke UOB Infinity, periksa apakah alamat website pada status bar di bagian atas browser Anda berubah dari **http://** ke **https://** dan **ikon keamanan ( )** muncul di samping kiri/kanan bar alamat URL browser Anda.

https://www.uob.co.id/corporate/infinity/index.page

Jika Anda tidak melihat simbol, segera tinggalkan website tersebut dan melaporkannya kepada UOB Call Centre di nomor **14008**.

Langkah tambahan untuk meningkatkan keamanan dalam transaksi online Anda

Jaga kerahasiaan ID pengguna dan Kata Sandi UOB Infinity Anda.

Ubah Kata Sandi Anda secara rutin.

Simpan Token Anda di tempat yang aman.

Segera laporkan kepada Bank jika Hard Token Anda rusak atau hilang.
Permintaan penggantian Hard Token yang rusak atau hilang harus disertai dengan formulir pengelolaan terkait. Dalam kondisi Hard Token rusak, Anda harus mengembalikan Hard Token rusak bersamaan dengan formulir pengelolaan tersebut kepada Bank.

Bank tidak pernah menanyakan data-data rahasia seperti PIN, kata sandi, login ID, data pribadi dan sebagainya melalui telepon, email ataupun aplikasi chat.

Unduh (download) aplikasi hanya dari situs yang terpercaya.
Sebaiknya Anda tidak mengakses atau bahkan mengunduh file dan/atau aplikasi dari website yang tidak dikenal atau tidak dapat diyakini keabsahannya.

Matikan Bluetooth atau Wi-Fi perangkat Anda terutama di tempat umum jika tidak digunakan.
Jangan melakukan koneksi internet melalui Wi-Fi publik yang tidak aman.

Selalu akses dengan mengetik https://infinity.uob.co.id/ dan tidak melalui tautan email ataupun chat
Kami sarankan untuk menyimpan akses UOB Infinity di menu favorit atau bookmarks.

Selalu logout dari UOB Infinity sebelum berpindah ke website lain dan pastikan selalu menghapus browser's disk cache.
(pada Menu Bar> pilih Tools> klik Delete Browsing History) terutama jika Anda mengakses rekening Anda dari terminal akses publik. Hal ini akan mencegah informasi rekening Anda tersimpan pada terminal.

Instal firewall personal[1] pada PC Anda sekaligus perangkat lunak (software) anti-virus dan anti-Malware[2] untuk melindungi PC Anda dari virus dan program yang berbahaya.

1 Firewall Personal
Firewall personal menyediakan dua fungsi dasar. Fungsi ini melindungi sistem Anda dari pemindai yang tidak diminta dari internet dan juga menawarkan kontrol ke luar. Pemindai ke dalam dapat mencari dan memblokir perintah, instruksi, program atau pesan yang tidak diundang masuk ke dalam sistem Anda; sementara kontrol ke luar akan mencari dan memblokir program yang tidak dikenal (seperti virus dan Malware) untuk mengirimkan pesan dari komputer Anda ke luar.

2 Malware
Malware dalam keamanan komputer merujuk kepada sebuah bentuk perangkat lunak yang mencurigakan (malicous software) yang dapat merusak sebuah sistem atau jaringan.
Tujuan dari Malware adalah memperoleh informasi dari target (kata sandi, kebiasaan pengguna yang tercatat dalam system log, data, dan lain-lain), dan mengendalikan target (memeroleh hak akses pada target).

Istilah Keamanan

Phising

Phising adalah tindakan dari pihak yang tidak bertanggung jawab dalam memperoleh informasi pribadi seperti *User ID, password*, atau informasi lainnya dengan tujuan penipuan dan bisa mengakibatkan akun internet banking dapat diakses oleh orang lain.

Cara kerja *phising* adalah memalsukan alamat website ataupun email. Tips agar terhindar dari *phising*:

- Pastikan kembali alamat *website* yang Anda kunjungi khususnya alamat *website* UOB Indonesia yaitu **uob.co.id**.
- Selalu update Sistem Operasi, *Software* aplikasi, dan *Browser* yang digunakan.
- Perhatikan alamat pengirim email dan pastikan kebenarannya sebelum melakukan tindakan apapun.
- Jangan membuka atau *download* lampiran apapun dari *email* yang tidak dikenal, karena lampiran tersebut kemungkinan berisi *malware*.
- Jangan sembarang klik *hyperlink* yang terdapat pada *hyperlink* bisa digunakan untuk mengarahkan Anda ke situs-situs *phising* yang berisi *malware* atau website yang meniipu pengguna agar memberikan informasi pribadi.

Malware

Malware adalah program atau *software* yang diciptakan untuk menyusup atau merusak sistem komputer yang bisa mengalihkan data hasil input nasabah/pengguna untuk kepentingan lainnya yang tidak bertanggung jawab sehingga bisa menyebabkan kerugian finansial terhadap nasabah.

Kerja *malware* hampir sama seperti virus, namun *malware* memberikan informasi dari komputer/perangkat kita ke server/asal *malware* tersebut.

Tips agar komputer/perangkat yang Anda pakai terhindar dari *malware*:

- Install perangkat anti *malware* dan lakukan update secara berkala.
- Selalu update Sistem Operasi, Software aplikasi, dan browser yang digunakan.
- Jangan sembarangan melakukan download dari internet dan pastikan dari situs terpercaya.

Jangan membuka email sembarangan dari orang yang tidak dikenal.

Social Engineering

Social Engineering adalah manipulasi psikologis dari seseorang dalam melakukan aksi atau menguak suatu informasi rahasia biasanya dilakukan melalui telepon atau internet. Oleh karena itu jangan pernah memberikan informasi sensitif mengenai akun bank Anda kepada orang lain.

Tips untuk menghindari Social Engineering :

- Selalu waspada pada saat berinteraksi di dunia nyata ataupun di dunia maya, apalagi jika berkaitan dengan informasi dimana Anda bekerja
- Jangan memberikan informasi sensitif mengenai pribadi ataupun tempat bekerja pada saat berinteraksi di dunia nyata ataupun dunia maya.

Virus

Virus adalah program komputer yang dibuat dan memiliki kemampuan untuk dapat merusak sistem operasi perangkat Anda, aplikasi, ataupun data yang ada pada perangkat tersebut.

Ciri-ciri komputer yang terkena virus :

- Komputer tidak stabil/sering hang
- Kinerja komputer terasa lambat
- Terdapat file aneh di dalam media penyimpanan komputer/perangkat yang kita gunakan.

Tips menghindari perangkat terkena virus :

- Install anti-virus.
- Update anti virus secara berkala
- Jangan install program dari sumber yang tidak dipercaya
- Selalu scan flashdisk atau media yang dikoneksikan ke perangkat Anda

Keylogger

Keylogger adalah program komputer yang dapat menyimpan apa yang Anda ketik di perangkat yang Anda gunakan.

Tips untuk menghindari dari Keylogger :

- Selalu gunakan perangkat yang biasa Anda pakai untuk bertransaksi dan pastikan tidak ada aplikasi yang Anda tidak pernah install
- Jangan menggunakan komputer/perangkat yang dipakai bersama untuk melakukan transaksi.

Hubungi Kami

Hubungi UOB Contact Center 14008 atau +62212355 9000 (dari luar negeri) untuk informasi lebih lanjut.

Right By You