Tips Aman Bertransaksi di Velocity@ocbcnisp
Safety Tips to Transact with Velocity@ocbcnisp

1. Umum

- Hindari mengakses Velocity@ocbcnisp menggunakan komputer atau jaringan WiFi publik (contoh: warnet, perpustakaan, kafe, dan tempat umum lainnya) yang tidak dapat dipastikan keamanannya.
- Lindungi komputer/*notebook* Anda dari ancaman *malware* (seperti *ransomware, trojan horse, worm*, dan lain-lain) dengan menggunakan *software* anti *malware*.
- Selalu perbaharui program anti *malware* Anda, serta lakukan proses *scan* secara berkala terhadap komputer/*notebook* Anda.
- Selalu menggunakan *software* resmi dan hindari *software* hasil bajakan ataupun *free software* pada komputer/*notebook* Anda.
- Jika ada aktivitas mencurigakan, segera laporkan ke Call OCBC NISP di 1500-999 atau +62-21-26506300 dari luar negeri, dan pilih Layanan "Nasabah Bisnis".

General

- *Avoid using public PC or WiFi access (e.g. cyber cafe, library, cafe, etc) which connection security is not guaranteed.*
- *Protect your PC/notebook from malicious software (e.g. ransomware, trojan horse, worm, etc) by using anti-malware software.*
- *Regulary scan and update the anti-malware software on your PC/notebook.*
- *Use official software only and avoid free or any kind of pirated softwares is not suggested for installation.*
- *Report any suspicious activites immediately to Call OCBC NISP at 1500-999 or +62-21-26506300 from overseas, and choose Service for "Business Banking Customers".*

2. ID Organisasi, ID Pengguna, Kata Sandi, dan PIN Token

- Ketika Anda mendaftar Velocity@ocbcnisp, Anda akan memperoleh ID Organisasi, ID Pengguna, dan kata sandi yang unik untuk Anda.
- Gunakan alamat *e-mail* resmi atau *e-mail* pribadi Anda untuk pendaftaran ID Pengguna dan pengiriman notifikasi transaksi.
- Ubah kata sandi secara berkala atau segera mengganti kata sandi setelah Anda merasa kata sandi diketahui oleh orang lain. Kata sandi Velocity@ocbcnisp terdiri atas minimum 8 dan maksimum 12 karakter (kombinasi minimal 1 huruf kapital, 1 huruf kecil, dan angka).
- Hindari membuat kata sandi dengan angka yang mudah dihubungkan dengan Anda, seperti nama, tanggal ulang tahun, atau nomor telepon.
- Jagalah kerahasiaan informasi ID Organisasi, ID Pengguna, kata sandi Velocity@ocbcnisp dan *e-mail*, serta PIN token Anda.
- Jangan menyimpan informasi ID Organisasi, ID Pengguna, kata sandi, PIN token Anda di dompet, telepon seluler, komputer/*notebook* dan sebagainya karena berisiko bila barang-barang tersebut hilang atau terinfeksi *malware*.
- Waspada upaya penipuan dari oknum yang mengaku sebagai petugas Bank OCBC NISP melalui telepon, faksimili, atau *e-mail* yang menanyakan data pribadi, termasuk kata sandi atau PIN Anda. Petugas Bank OCBC NISP tidak pernah meminta atau menanyakan kata sandi atau PIN Anda.
- Jika ID Organisasi, ID Pengguna, dan kata sandi atau PIN Anda diketahui orang lain/dicuri/hilang, segera lakukan pemblokiran terhadap akun Anda dengan menghubungi Call OCBC NISP di 1500-999 atau +62-21-26506300 dari luar negeri, dan pilih Layanan "Nasabah Bisnis".

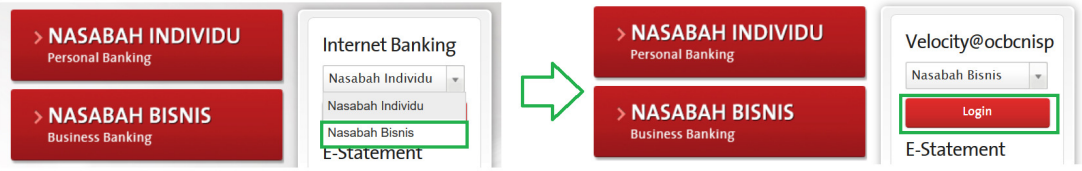
Organization ID, User ID, Password, and Token PIN

- *Upon Velocity@ocbcnisp registration, you will receive a unique Organization ID, User ID, and password.*
- *Use an official or personal e-mail address for account registration and for transaction notification.*

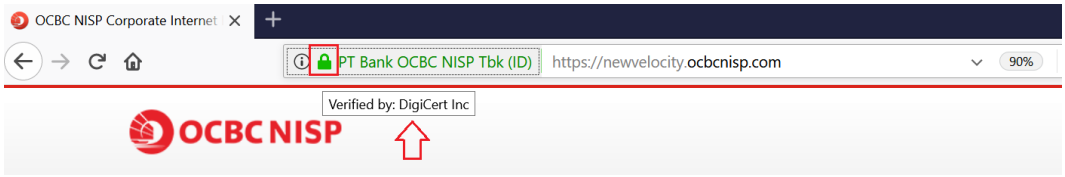
- *Update your password regularly or as soon as your password is discovered by any other parties. Velocity@ocbcnisp password must consist of a minimum of 8 to 12 characters the most (a combination of 1 upper case letter, 1 lower case letter, and a number).*
- *Avoid password that consists of anything closely related to your personal information (e.g. name, birth date, or phone number).*
- *Keep your Velocity@ocbcnisp Organization ID, User ID, password, and Token PIN confidential.*
- *Don't keep your Organization ID, User ID, password, and Token PIN information in your wallet, cellphone, PC/notebook that has potential risks for lost or malware attacks.*
- *Be aware of fraudulent practice that falsely purport to be associated with OCBC NISP, asking for personal information, including password and PIN, via phone, facsimile, or e-mail. OCBC NISP associates will never ask for your password or PIN.*
- *If your Organization ID, User ID, password, or PIN is discovered/stolen/lost, block immediately by contacting Call OCBC NISP at 1500-999 or +62-21-26506300 from overseas, and choose Service for "Business Banking Customers".*

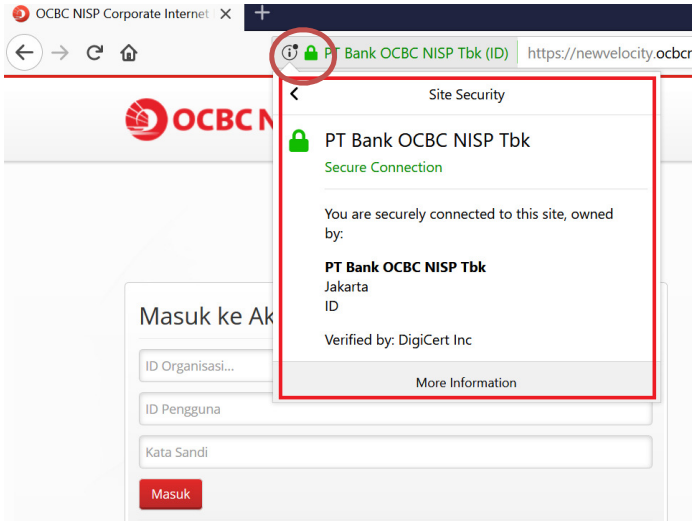
3. Halaman Akses

- Pastikan Anda mengakses Velocity@ocbcnisp melalui situs resmi Bank OCBC NISP di www.ocbcnisp.com, kemudian pilihbagian "Internet Banking", "Nasabah Bisnis" atau langsung login ke halaman Velocity@ocbcnisp di https://newvelocity.ocbcnisp.com.



- Pastikan terdapat ikon gembok/kunci pada *browser* Anda, dimulai pada halaman login. Hal ini mengindikasikan bahwa halaman yang Anda akses saat ini aman dan sudah dienkripsi.

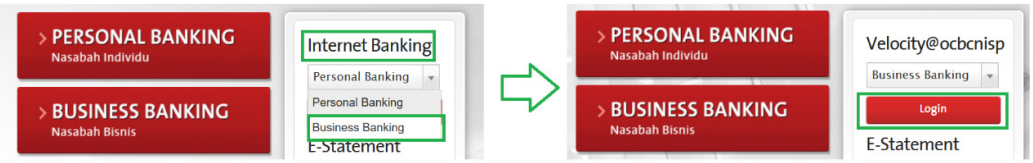




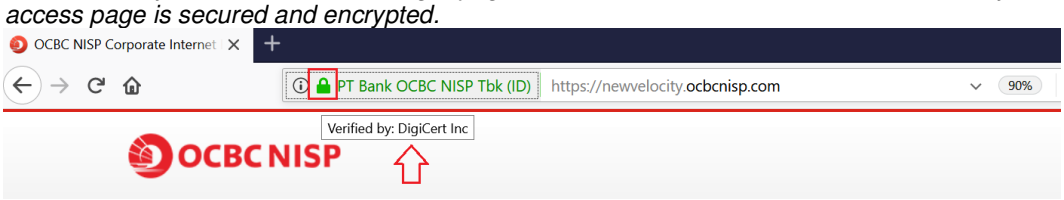
- Pastikan alamat situs Velocity@ocbcnisp yang Anda tulis di *browser* sudah benar. Untuk menghindari kesalahan penulisan alamat situs Velocity@ocbcnisp, simpan alamat situs pada menu *favorites* atau *bookmarks*, sehingga untuk selanjutnya Anda cukup memilih dari menu tersebut.
- Pastikan nama dan nomor rekening penerima serta bank tujuan sudah benar, ketika Anda melakukan transaksi melalui Velocity@ocbcnisp.
- Token Velocity@ocbcnisp hanya digunakan untuk melakukan transaksi finansial. Waspada jika ada permintaan untuk memasukan kode jawaban (*response code*) token selain untuk transaksi finansial.
- Lakukan pengecekan riwayat transaksi Anda secara berkala.
- Jangan meninggalkan komputer/*notebook* anda dalam kondisi Velocity@ocbcnisp masih aktif. Pastikan Anda selalu *log out* setelah selesai menggunakan Velocity@ocbcnisp.

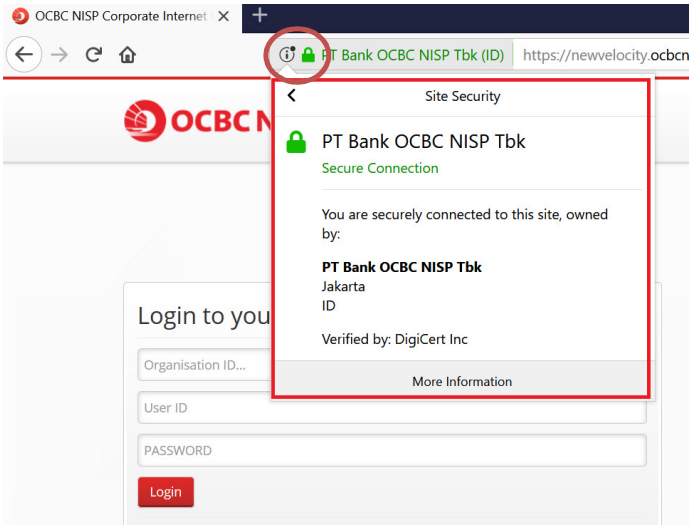
Login Page

- *Be sure that you access Velocity@ocbcnisp through the official website of OCBC NISP at www.ocbcnisp.com. On the "Internet Banking" section, choose "Business Banking" or go directly to Velocity@ocbcnisp login page at https://newvelocity.ocbcnisp.com.*



- *Be sure that your browser on the login page shows a lock icon. This will indicate that your access page is secured and encrypted.*





- *Be sure that Velocity@ocbcnisp web address is correct when do login. To avoid any mispelling of Velocity@ocbcnisp website address, save it to your favorites or bookmarks menu. You can directly access Velocity@ocbcnisp from this menu anytime.*

- *When do any transaction through Velocity@ocbcnisp, be sure that the beneficiary name, account number, and the bank destination are input correctly.*
- *Velocity@ocbcnisp Token is used upon financial transactions only. Be aware of any response-code request other than for financial transaction purposes.*
- *A periodical transaction history checking is highly suggested.*
- *Don't leave your PC/notebook while Velocity@ocbcnisp is still active. Be sure to log out after finish using Velocity@ocbcnisp.*

4. *Phishing*

Phishing adalah modus kejahatan di dunia maya yang bertujuan untuk mendapatkan informasi pribadi seseorang seperti ID Pengguna, kata sandi, PIN, maupun nomor rekening secara tidak sah. *Phishing* dapat dilakukan melalui berbagai media komunikasi elektronik seperti *e-mail,* pesan instan, telepon, SMS, dan lain-lain.

Beberapa teknik penipuan *phishing* yang biasa dilakukan:

- Menggunakan alamat *e-mail* palsu untuk meminta informasi rahasia dengan berbagai alasan, misalnya perbaikan sistem maupun *upgrade*.
- Menggunakan situs web palsu yang mirip dengan yang asli. Biasanya pelaku *phishing* membuat situs web palsu dengan nama yang sama namun *domain* berbeda atau bisa dengan alamat URL yang diubah satu sampai dua huruf.
- Mengirimkan form isian melalui *e-mail* atau menghubungi melalui telepon dengan mengaku sebagai pihak Bank untuk meminta informasi ID Pengguna, kata sandi atau PIN.
- Mengirimkan *link* yang bertujuan untuk mengarahkan ke suatu situs web tertentu, yang merupakan situs web palsu.

Langkah pencegahan *phishing*:

- Pastikan kebenaran alamat pengirim *e-mail* dan web sebelum memberikan respon.
- Selalu waspada dan jangan membuka *link* serta mengisi informasi pribadi Anda, jika *e-mail* atau situs web mencurigakan.
- Jangan terpancing untuk menyebutkan identitas atau informasi rahasia lainnya, jika Anda menerima panggilan dari nomor yang tidak dikenal.

Phishing

Phishing is a fraudulent practice in cyber world that induces to reveal personal information such as User ID, password, and PIN for scam purposes. Phishing is commonly done via electronic communications (e.g. e-mails, texts, etc).

A few of phishing techniques that are commonly used:

- *Using a false e-mail address to request for confidential information upon various purposes, such as for repair or system upgrade.*
- *Using a false website address that is similar to the official one. Phishing perpetrators would make a fake address with a same name, but with a different domain or with a URL which address has been tweaked one to two letters.*
- *Sending forms through e-mail or contacting the victims via phone calls by purpoting to be a Bank official in order to request for a User ID, password, or PIN.*
- *Sending a link that is used to bait victims to click on, and later direct them to a scam website.*

How to prevent phishing:

- *Be sure to always check the legitimacy of an e-mail or a website address before proceeding with any further response.*
- *Be alert by not click any suspicious links or submit any confidential information to an unrecognized e-mail address.*
- *Don't reveal any ID or other confidential information if you receive a call from an unknown caller ID.*