Tips Aman Bertransaksi di OCBC Business
Safety Tips to Transact with OCBC Business

1. Umum

- Hindari mengakses OCBC Business menggunakan komputer/perangkat *mobile* yang disediakan di tempat umum menggunakan jaringan WiFi publik (contoh: warnet, perpustakaan, kafe, dan tempat umum lainnya) yang tidak dapat dipastikan keamanannya.
- Lindungi komputer/perangkat *mobile* Anda dari ancaman *malware* (seperti *ransomware, trojan horse, worm*, dan lain-lain) dengan menggunakan *software* anti *malware*. Gunakan Kata Sandi/PIN untuk mengamankan akses ponsel/perangkat *mobile* Anda.
- Jika komputer/perangkat *mobile* Anda perlu diakses oleh pengguna lain, atau akan diperbaiki:
    - Pastikan Anda tidak menyimpan informasi kredensial *login* seperti nomor rekening, ID Organisasi, ID Pengguna, Kata Sandi/PIN, dan lain-lain dalam komputer/perangkat *mobile* Anda.
    - Hapus *cache* dan *temporary files* yang tersimpan dalam komputer/perangkat *mobile* Anda, karena mungkin mengandung nomor rekening dan informasi rahasia lainnya.
    - Hapus informasi yang tersimpan dalam fitur pengisian data otomatis dalam komputer/perangkat *mobile* Anda.
- Selalu perbarui program anti *malware* Anda, serta lakukan proses *scan* secara berkala terhadap komputer/perangkat *mobile* Anda. Untuk perangkat *mobile*, pastikan sistem operasi *(OS)* perangkat Anda selalu diperbarui dengan peningkatan keamanan terbaru.
- Selalu menggunakan *software* resmi dan hindari *software* hasil bajakan ataupun *free software* pada komputer/perangkat *mobile* Anda.
- Jangan menggunakan perangkat *mobile* yang telah di-*jailbreak*/*rooting* untuk mengakses OCBC Business mobile. *Jailbreaking/rooting* akan mengekspos perangkat Anda kepada *malware* yang dapat membahayakan keamanan data Anda.
- Daftarkan/perbarui nomor ponsel dan *e-mail* Anda kepada Bank untuk notifikasi aktivitas transaksi Anda. Jika ada aktivitas mencurigakan, atau jika Anda kehilangan perangkat Anda, segera laporkan ke TANYA OCBC di 1500-999 atau +62-21-26506300 dari luar negeri, dan pilih Layanan “Nasabah Bisnis”.

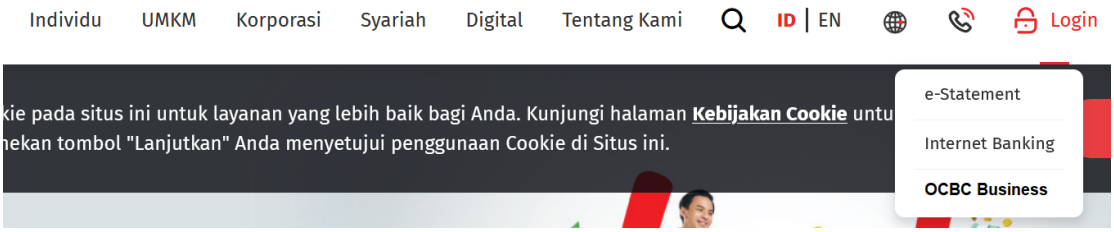
General

- *Avoid using public PC/mobile device using an unsecured WiFi access (e.g. cyber cafe, library, cafe, etc) where connection security may be compromised.*
- *Protect your PC/mobile device from malicious software (e.g. ransomware, trojan horse, worm, etc) by using anti-malware software. Set up a Password/PIN to prevent unauthorised access to your mobile device.*
- *If your PC/mobile device is accessed by multiple users, or about to be sent out for repairs:*
    - *Ensure that you do not save login credentials such as your account number, Organization ID, User ID, PIN/Password, and others in your device.*
    - *Clear cache and temporary files stored in your device, as they may contain account numbers and other sensitive information.*
    - *Delete all information stored in your device’s auto-fill feature.*
- *Regulary scan and update the anti-malware software on your PC/mobile device. For mobile devices, ensure your device’s operating system (OS) are always updated with the latest security updates.*
- *Use official software only and avoid free or any kind of pirated softwares is not suggested for installation.*
- *Do not use jailbroken/rooted device to access OCBC Business mobile. Jailbreaking/rooting will expose your device to malwares that may compromise your data security.*
- *Register/update your mobile number and e-mail ID for notifications of your transaction activities. Report any suspicious activities or device loss immediately to TANYA OCBC at 1500-999 or +62-21-26506300 from overseas and choose Service for “Business Banking Customers”.*

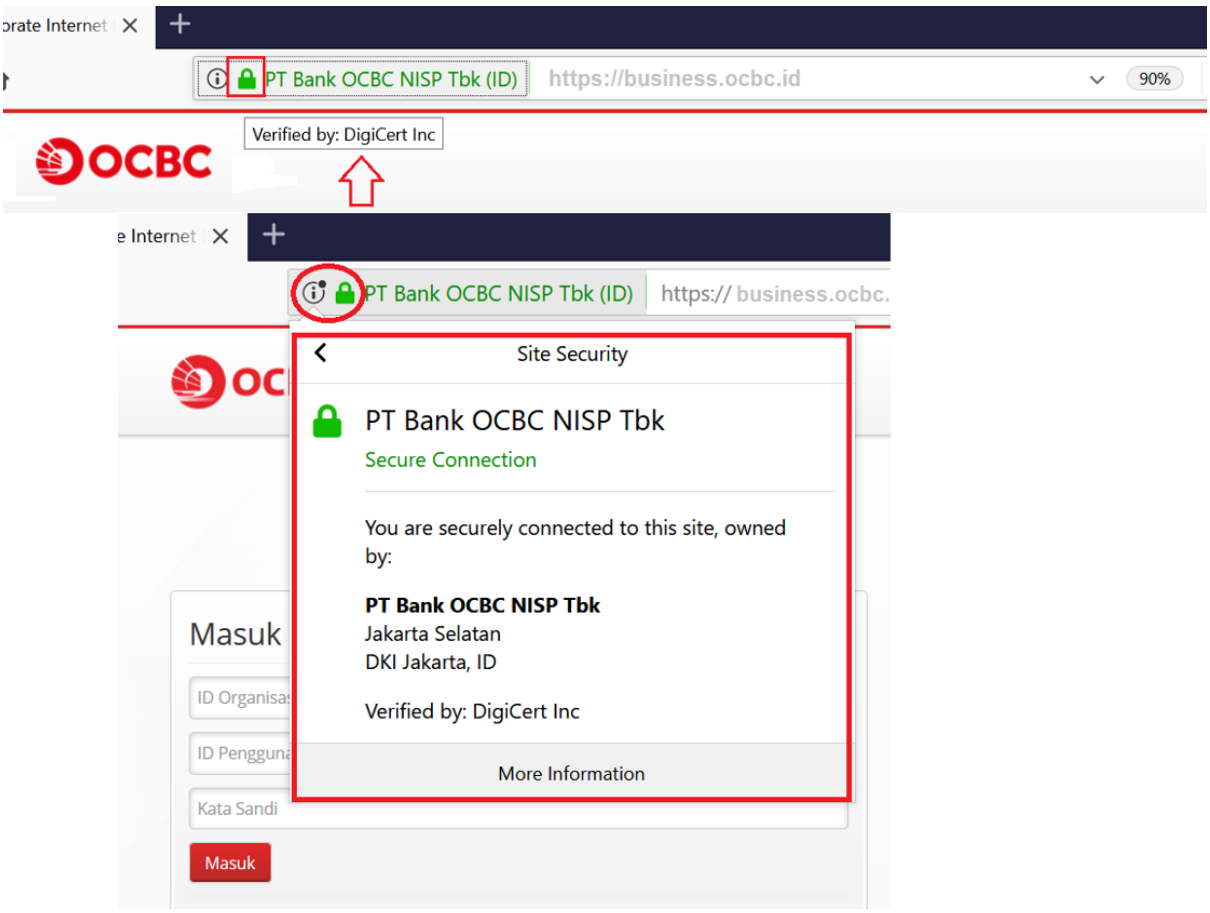
OCBC Information Classification: Public

2. Halaman Akses

- Pastikan Anda mengakses OCBC Business melalui situs resmi OCBC di https://www.ocbc.id, kemudian pilih bagian “Login – OCBC Business” atau langsung *login* ke halaman OCBC Business di https://business.ocbc.id.



- 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.



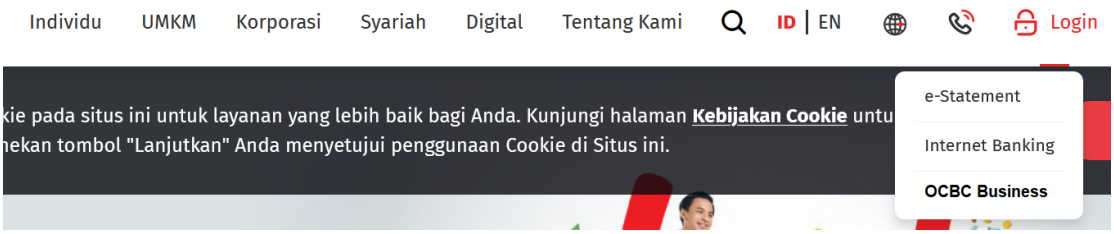
- Pastikan alamat situs OCBC Business yang Anda tulis di *browser* sudah benar. Untuk menghindari kesalahan penulisan alamat situs OCBC Business, simpan alamat situs pada menu *favorites* atau *bookmarks*, sehingga untuk selanjutnya Anda cukup memilih dari menu tersebut.
- Pastikan nama dan nomor rekening penerima serta Bank tujuan sudah benar, ketika Anda melakukan transaksi melalui OCBC Business.
- Token OCBC Business 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.

OCBC Information Classification: Public

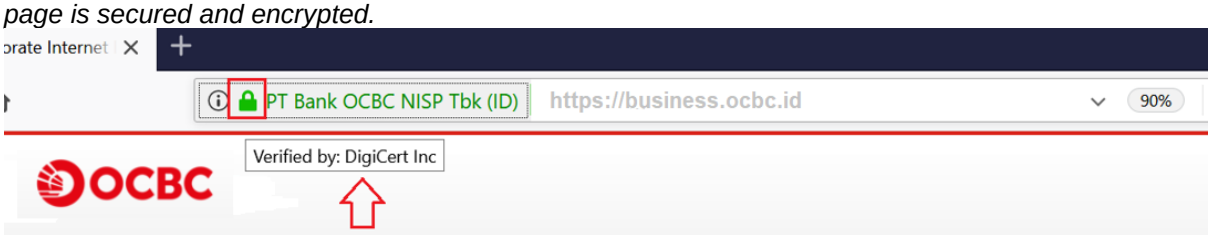
- Jangan meninggalkan komputer, *notebook,* atau perangkat *mobile* Anda dalam kondisi OCBC Business masih aktif. Pastikan Anda selalu *log out* setelah selesai menggunakan OCBC Business.

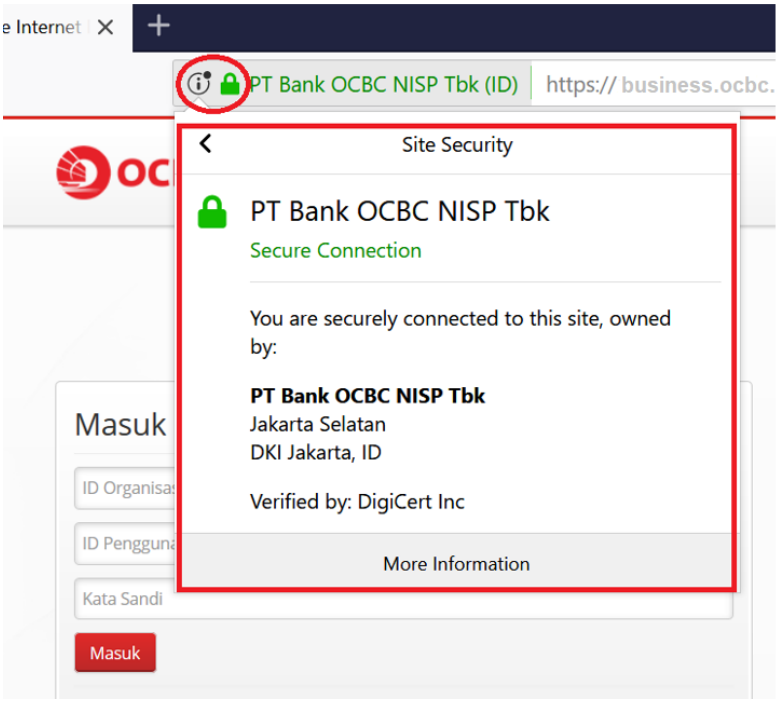
Login Page

- *Ensure that you access OCBC Business through the official website of OCBC at* https://www.ocbc.id*. On the "Login – OCBC Business" section or go directly to OCBC Business login page at https://business.ocbc.id.*



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





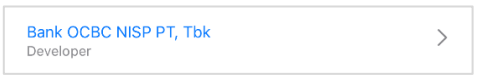
- *Ensure that OCBC Business web address is correct when do login. To avoid any misspelling of OCBC Business website address, save it to your favorites or bookmarks menu. You can directly access OCBC Business from this menu anytime.*
- *When do any transaction through OCBC Business, ensure that the beneficiary name, account number, and the Bank destination are inputted correctly.*
- *The OCBC Business token is only used for financial transactions. Be alert if there is a request to enter the response code token in addition to financial transactions.*

OCBC Information Classification: Public

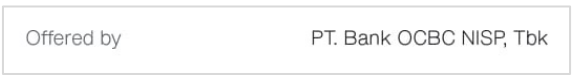
- *A periodical transaction history checking is highly suggested.*
- *Don't leave your PC, notebook, or mobile device while OCBC Business is still active. Ensure to log out after finish using OCBC Business.*

3. Unduh Aplikasi

- Pastikan penerbit aplikasi adalah **PT Bank OCBC NISP, Tbk.**



Penerbit aplikasi di Apple App Store (iOS)

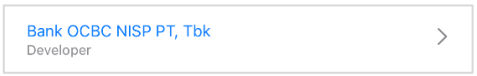


Penerbit aplikasi di Google Play Store (Android)

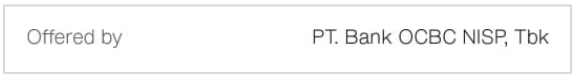
- Deskripsi aplikasi dapat berubah sewaktu-waktu mengikuti pembaruan terkini, namun secara umum deskripsi aplikasi seharusnya tidak memiliki banyak kesalahan penulisan serta menjelaskan fungsi aplikasi secara jelas.
- Selalu perbarui aplikasi Anda jika diminta dalam bentuk notifikasi saat *login.*

Downloading the App

- *Verify the application publisher is **PT Bank OCBC NISP, Tbk.***



App publisher on Apple App Store (iOS)



App publisher on Google Play Store (Android)

- *App description may change at any time follow the latest updates, however in general it should not have many misspelling and explain the functionality of the application clearly.*
- *Always update your app when prompted via notification upon logging in.*

4. Otorisasi Token

- OCBC Business memiliki dua pilihan token untuk otorisasi transaksi: dalam bentuk perangkat keras *(Hardware Token)* untuk transaksi via *web* dan *mobile*, dan perangkat lunak *(Software Token)* untuk transaksi via *mobile.*
- Token OCBC Business hanya digunakan untuk melakukan transaksi finansial. Waspada jika ada permintaan untuk memasukan kode jawaban (*response code*) token selain untuk transaksi finansial.
- Pastikan Anda membaca dengan seksama Syarat dan Ketentuan *Software Token* yang ditampilkan saat pembuatan pada aplikasi *mobile* Anda.
- Jika perangkat atau nomor ponsel dicuri atau hilang, atau diduga disalahgunakan pihak lain, segera blokir *Software Token* dengan cara menghubungi TANYA OCBC 1500-999 atau kantor cabang terdekat.

Token Authorization

- *OCBC Business offers two token options for transaction authorization purposes: Hardware Token for web and mobile transactions, and Software Token for mobile transactions.*
- *OCBC Business Token is used upon financial transactions only. Be aware of any response code request other than for financial transaction purposes.*
- *Ensure that you have thoroughly reviewed Software Token Terms and Conditions shown during token creation in your mobile app.*
- *In the event of stolen or loss of device and/or phone number, or suspected abuse by another party, immediately contact TANYA OCBC 1500-999 or your nearest Branch Office to block your Software Token.*

OCBC Information Classification: Public

5. *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,* SMS*,* aplikasi *chatting online*, 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 biasanya merupakan situs web palsu.

Langkah pencegahan *phishing*:

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

Phishing

Phishing is a fraudulent attempt in cyber world to obtain personal information such as User ID, Password, PIN, and account number for scam purposes. Phishing is commonly done via electronic communications (e.g. e-mails, texts, etc).

Several 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, SMS, online messenger apps, or contacting the victims via phone calls by purpoting to be a Bank official in order to request for a User ID, Oassword, 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:

- *Ensure to always check the legitimacy of an e-mail, SMS, a website address, or other communication media before proceeding with any further response.*
- *Stay alert and do 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*

6. Aplikasi Palsu

Aplikasi palsu adalah aplikasi tiruan yang dibuat mirip dengan aplikasi resmi, namun berisi *malware* yang bertujuan untuk mencuri data pribadi/sensitif, atau informasi kredensial perbankan Anda. Aplikasi palsu ini didesain dengan tampilan yang serupa dengan aplikasi aslinya dengan cara menggunakan gambar dan ikon yang sama, serta meniru nama penerbit aplikasi.

OCBC Information Classification: Public

Cara mencegah pengunaan aplikasi palsu:

- Pastikan aplikasi OCBC Business mobile diunduh dari Apple iOS App Store dan Android Google Play Store resmi perangkat Anda. Bank tidak mengizinkan publikasi aplikasi dari *application marketplace* lain.
- Sebelum mengunduh aplikasi baru, cek penerbit aplikasi yaitu **PT Bank OCBC NISP, Tbk.**, dan pastikan Anda membaca deskripsi aplikasi secara seksama. Aplikasi palsu biasanya akan tidak memiliki deskripsi atau memiliki deskripsi yang tidak ada hubungannya dan biasanya memiliki kesalahan penulisan.
- Pastikan Anda membaca syarat dan ketentuan dengan seksama. Beberapa aplikasi palsu mungkin memiliki syarat dan ketentuan yang terlihat sah.
- Aplikasi palsu dapat menguras baterai perangkat Anda dengan cepat, sehingga baterai yang terus-menerus cepat habis dapat menjadi menandakan infeksi *malware* atau virus.

Rogue Apps

Rogue apps are illegitimate "look-alike" apps with embedded malware with an intention to steal sensitive/critical data or banking credentials. These apps are designed to look like real mobile banking apps, such as using the same images, icons, and closely imitating the publisher's name.

How prevent downloading rogue mobile banking apps:

- *Only download OCBC Business mobile apps from the official Apple iOS App store and Android Google Play store. No other app stores are authorised to carry apps developed by Bank.*
- *Before downloading a new app, always check the publisher, which should be **PT Bank OCBC NISP, Tbk.,** and read the app description carefully. Rogue apps will usually contain irrelevant/no description about the app functionality and a lot of misspellings.*
- *Ensure to read the legal terms and conditions carefully. Some rogue mobile apps may come with a well-written legal term that makes it seem legit.*
- *Rogue apps can drain phone batteries fast, so battery running low frequently indicate a malware or virus infection.*

7. *SIM Swap*

SIM Swap adalah modus kejahatan dimana pelaku mengambil alih nomor ponsel Anda dengan cara menggunakan identitas palsu untuk meminta operator jaringan mencetak kartu SIM baru, sehingga memperoleh akses OTP dan *push notification* Anda. Metode ini dapat membahayakan sistem pengamanan 2 faktor otentikasi yang telah diimplementasi oleh aplikasi OCBC Business mobile.

Untuk melindungi diri Anda dari *SIM Swap*:

- Waspada dengan upaya-upaya *phishing* dan jangan mengunduh aplikasi palsu dimana pelaku akan memperoleh informasi perbankan dan identitas Anda.
- Daftarkan nomor ponsel Anda untuk *push notification* untuk selalu memantau transaksi perbankan Anda.
- Jika Anda mengalami gangguan seperti tidak bisa menerima panggilan, pesan, ataupun OTP, segera verifikasi kepada pihak penyedia jasa seluler Anda dan kepada Bank untuk memblokir akses perbankan dengan nomor ponsel Anda. Hal tersebut dapat terjadi karena pelaku berhasil memperoleh SIM card baru untuk nomor Anda, sehingga SIM card lama anda dinonaktifkan.
- Jangan menonaktifkan/memasang mode *silent* pada nomor ponsel Anda jika menerima banyak panggilan menganggu, karena hal tersebut dapat menjadi cara penipu untuk mengalihkan Anda menjadi agar tidak menyadari status jaringan nomor ponsel Anda yang dinonaktifkan. Abaikan saja panggilan-panggilan tersebut.

SIM Swap

SIM Swap is a fraudulent practice where the fraudster takes over your phone number by requesting a new SIM card to your network operator using a fake identity, thus gaining access to your OTPs and push notifications. This method may compromise the 2-factor authentication security system implemented by OCBC Business mobile.

OCBC Information Classification: Public

<u>To prevent exposure to SIM swap fraud:</u>

- *Be aware towards phishing methods, and refrain from downloading rogue apps, in which the fraudster may gain information of your banking credentials and personal identity.*
- *Register your cell phone number for push notifications to monitor your banking transactions.*
- *If you notice that you are unable to receive calls, texts, or OTPs, immediately contact your cellular network provider and to the Bank to block your phone number banking access. This may happen when the fraudster obtained a new SIM card of your cell phone number, thus deactivating your current SIM card.*
- *Do not switch off/setting your phone on silent mode, even when you are receiving numerous annoying call, because this could be a ploy to divert you to being unaware that your cellular network is being deactivated. Ignore these calls instead.*

OCBC Information Classification: Public