Panduan Pengguna | User Guide I 指南
OCBC Business

Tips Aman Bertransaksi | Safe Transaction Tips | 安全交易提示

Panduan ini bersifat informatif dan disediakan sebagai referensi umum bagi Nasabah OCBC. Nasabah bertanggung jawab untuk menjaga kerahasiaan data pribadi, kredensial login, serta keamanan perangkat yang digunakan dalam mengakses OCBC Business. Informasi yang tercantum dalam panduan ini dapat berubah sewaktu-waktu tanpa pemberitahuan sebelumnya.

This guide is provided for informational purposes only and serves as a general reference for OCBC customers. Customers are responsible for maintaining the confidentiality of their personal data, login credentials, and the security of devices used to access OCBC Business. The information contained in this guide is subject to change without prior notice.

本指南仅供参考，作为 OCBC 客户的一般信息说明。客户有责任妥善保管个人资料、登录凭证，并确保用于访问 OCBC Business 的设备安全。本指南所载信息可能随时更改，恕不另行通知。

Umum | General | 一般安全提示

1. **[ID]** Hindari mengakses OCBC Business menggunakan komputer/perangkat mobile yang disediakan di tempat umum atau menggunakan jaringan WiFi publik (contoh: warnet, perpustakaan, kafe, dan tempat umum lainnya) yang tidak dapat dipastikan keamanannya.

   [EN] Avoid accessing OCBC Business using public computers/mobile devices or unsecured public WiFi networks (e.g. cyber cafés, libraries, cafés, and other public places) where the security of the connection cannot be assured

   [CN] 请避免使用公共场所提供的电脑/移动设备或通过安全性无法保证的公共 WiFi 网络（例如网吧、图书馆、咖啡馆及其他公共场所）访问 OCBC Business。

2. **[ID]** 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.

   [EN] Protect your computer/mobile device from malware (such as ransomware, trojan horses, worms, etc.) by using anti-malware software. Set up a Password/PIN to secure access to your mobile device.

   [CN] 请使用反恶意软件保护您的电脑/移动设备免受恶意软件（如勒索软件、木马、蠕虫等）的威胁。请设置密码/PIN，以保护您的手机/移动设备免遭未经授权的访问。

3. **[ID]** 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.

   [EN] If your computer/mobile device needs to be accessed by another user or sent for repair, ensure that you do not store login credentials such as your account number, Organization ID, User ID, Password/PIN, and other confidential information on your device.

   [CN] 如果您的电脑/移动设备需要由其他用户使用或送修，请确保设备中未保存账户号码、Organization ID、User ID、密码/PIN 及其他登录凭证。

4. **[ID]** Hapus cache dan temporary files yang tersimpan dalam komputer/perangkat mobile Anda karena mungkin mengandung nomor rekening dan informasi rahasia lainnya.

   [EN] Clear cache and temporary files stored on your computer/mobile device, as they may contain account numbers and other confidential information.

   [CN] 请清除电脑/移动设备中存储的缓存和临时文件，因为其中可能包含账户号码及其他机密信息。

5. **[ID]** Hapus informasi yang tersimpan dalam fitur pengisian data otomatis dalam komputer/perangkat mobile Anda.

   [EN] Delete all information stored in your computer/mobile device's auto-fill feature.

[CN] 请删除电脑/移动设备自动填充功能中保存的信息。

6. [ID] 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.

   [EN] Regularly scan and update the anti-malware software on your computer/mobile device. For mobile devices, ensure that your device's operating system (OS) is always updated with the latest security updates.

   [CN] 请定期扫描您的电脑/移动设备并更新反恶意软件。对于移动设备，请确保设备的操作系统 (OS) 始终更新至包含最新安全更新的版本。

7. [ID] Selalu menggunakan software resmi dan hindari software hasil bajakan ataupun free software pada komputer/perangkat mobile Anda.

   [EN] Always use official software and avoid pirated software or free software on your computer/mobile device.

   [CN] 请始终使用官方正版软件，并避免在电脑/移动设备上使用盗版软件或免费软件。

8. [ID] 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.

   [EN] Do not use a jailbroken/rooted mobile device to access OCBC Business mobile. Jailbreaking/rooting may expose your device to malware that can compromise your data security.

   [CN] 请勿使用已越狱 (jailbroken) 或已获取 Root 权限的移动设备访问 OCBC Business mobile。越狱或 Root 可能使您的设备暴露于恶意软件威胁，并危及您的数据安全。

9. [ID] Daftarkan/perbarui nomor ponsel dan email Anda kepada Bank untuk notifikasi aktivitas transaksi Anda. Apabila Anda menemukan aktivitas yang mencurigakan atau membutuhkan klarifikasi lebih lanjut, mohon segera menghubungi Relationship Manager Anda atau hubungi TANYA OCBC 1500-999 atau +62-21-26506300 dari luar negeri (pilih #2 untuk Layanan Nasabah Bisnis), WhatsApp ke 08121500999, email ke clientservices@ocbc.id.

   [EN] Register/update your mobile number and email address with the Bank to receive notifications of your transaction activities. If you notice any suspicious activity or require further clarification, please immediately contact your Relationship Manager or TANYA OCBC at 1500-999 or +62-21-26506300 from overseas (select #2 for Business Customer Service), WhatsApp at 08121500999, or email clientservices@ocbc.id.

   [CN] 请向银行登记/更新您的手机号码和电子邮箱，以接收交易活动通知。如发现任何可疑活动或需要进一步确认，请立即联系您的客户经理 (Relationship Manager)，或拨打 TANYA OCBC 1500-999；如从海外拨打，请拨 +62-21-26506300（选择 #2 企业客户服务），也可通过 WhatsApp 08121500999 或发送电子邮件至 clientservices@ocbc.id 联系我们。

Halaman Akses | Login Page | 登录页面

1. **[ID]** Pastikan Anda mengakses OCBC Business melalui situs resmi OCBC Business di https://www.ocbc.id, kemudian pilih bagian "Login – OCBC Business" atau langsung login ke halaman OCBC Business web di https://business.ocbc.id atau aplikasi OCBC Business mobile.

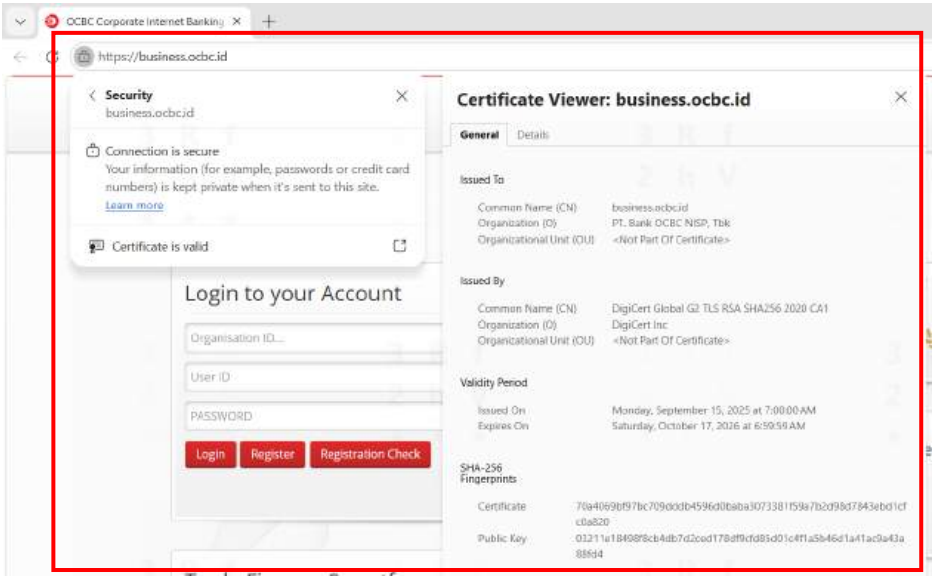
   [EN] Ensure that you access OCBC Business through the official OCBC website at https://www.ocbc.id. Select the "Login – OCBC Business" section, or go directly to the OCBC Business web login page at https://business.ocbc.id or use the OCBC Business mobile app.

   [CN] 请确保通过 OCBC 官方网站 https://www.ocbc.id 访问 OCBC Business，然后选择"Login – OCBC Business"，或直接通过 https://business.ocbc.id 登录 OCBC Business 网页版，亦可使用 OCBC Business mobile 应用程序。

2. **[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.

   [EN] Ensure that your browser displays a lock icon starting from the login page. This indicates that the page you are accessing is secure and encrypted.

   [CN] 从登录页面开始，请确保您的浏览器显示锁形图标。这表示您当前访问的页面是安全且经过加密的



OCBC Information Classification: Public

3. **[ID]** 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.

   [EN] Ensure that the OCBC Business website address entered in your browser is correct. To avoid mistyping the OCBC Business website address, save it to your favorites or bookmarks so that you can access it directly from the menu in the future.

   [CN] 请确保您在浏览器中输入的 OCBC Business 网站地址正确。为避免输错 OCBC Business 网站地址，请将其保存至浏览器的收藏夹或书签，以便日后直接从该菜单访问。

4. **[ID]** Pastikan nama dan nomor rekening penerima serta Bank tujuan sudah benar ketika Anda melakukan transaksi melalui OCBC Business.

   [EN] When performing a transaction through OCBC Business, ensure that the beneficiary name, account number, and destination Bank are entered correctly.

   [CN] 通过 OCBC Business 进行交易时，请确保收款人姓名、账户号码及收款银行信息均输入正确。

5. **[ID]** Token OCBC Business hanya digunakan untuk melakukan transaksi finansial. Waspada jika ada permintaan untuk memasukkan kode jawaban (response code) token selain untuk transaksi finansial.

   [EN] The OCBC Business Token is only used for financial transactions. Be alert if you are requested to enter a Token response code for purposes other than financial transactions.

   [CN] OCBC Business Token 仅用于金融交易。如有人要求您为金融交易以外的用途输入 Token 响应码 (response code)，请提高警惕。

6. **[ID]** Lakukan pengecekan riwayat transaksi Anda secara berkala.

   [EN] Check your transaction history regularly.

   [CN] 请定期检查您的交易记录。

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

   [EN] Do not leave your computer, notebook, or mobile device unattended while OCBC Business is still active. Always log out after you have finished using OCBC Business.

   [CN] 当 OCBC Business 仍处于登录状态时，请勿让您的电脑、笔记本电脑或移动设备处于无人看管状态。使用完 OCBC Business 后，请务必退出登录。

Unduh Aplikasi | Downloading the App | 下载应用程序

1. **[ID]** Pastikan penerbit aplikasi adalah PT Bank OCBC NISP, Tbk.

   [EN] Verify that the application publisher is PT Bank OCBC NISP, Tbk.

   [CN] 请确认应用程序的发布者为 PT Bank OCBC NISP, Tbk.

Penerbit Aplikasi | App Publisher | 应用程序发布者
— Apple App Store (iOS)

Penerbit Aplikasi | App Publisher | 应用程序发布者
— Google Play Store (Android)

2. **[ID]** 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.

   [EN] The app description may change from time to time following the latest updates. However, in general, the app description should not contain many spelling errors and should clearly explain the application's functionality.

   [CN] 应用程序的描述可能会随最新更新而不时变更，但通常情况下，应用程序描述不应存在大量拼写错误，并应清楚说明应用程序的功能。

3. **[ID]** Selalu perbarui aplikasi Anda jika diminta dalam bentuk notifikasi saat login.

   [EN] Always update your app when prompted via a notification upon logging in.

   [CN] 登录时如收到应用程序更新通知，请及时更新您的应用程序。

Otorisasi Token | Token Authorization | Token 授权

1. **[ID]** 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.

   [EN] OCBC Business offers two token options for transaction authorization: Hardware Token for web and mobile transactions, and Software Token for mobile transactions.

   [CN] OCBC Business 提供两种用于交易授权的 Token：Hardware Token，可用于网页端和移动端交易；以及 Software Token，可用于移动端交易。

2. **[ID]** Token OCBC Business hanya digunakan untuk melakukan transaksi finansial. Waspada jika ada permintaan untuk memasukkan kode jawaban (response code) token selain untuk transaksi finansial.

   [EN] The OCBC Business Token is only used for financial transactions. Be alert if you are requested to enter a Token response code for purposes other than financial transactions.

   [CN] OCBC Business Token 仅用于金融交易。如有人要求您为金融交易以外的用途输入 Token 响应码 (response code)，请提高警惕。

3. **[ID]** Pastikan Anda membaca dengan saksama Syarat dan Ketentuan Software Token yang ditampilkan saat pembuatan pada aplikasi mobile Anda.

   [EN] Ensure that you carefully read the Software Token Terms and Conditions displayed during token creation in your mobile app.

   [CN] 在移动应用程序中创建 Software Token 时，请仔细阅读所显示的 Software Token 条款与条件。

4. **[ID]** Jika perangkat atau nomor ponsel dicuri atau hilang, atau diduga disalahgunakan pihak lain, lakukan langkah berikut.
   a. Blokir Software Token Anda
      Anda dapat mengirimkan email permohonan ke clientservices@ocbc.id dengan menggunakan alamat email Anda yang terdaftar di sistem OCBC Business. Informasikan ID Organisasi, ID Pengguna, dan jenis Token misalnya Token Software.
   b. Blokir Akses Pengguna
      - OCBC Business web: klik **Blokir User Saya** pada halaman login OCBC Business web (https://business.ocbc.id) dan ikuti instruksi yang tertera pada layar.
      - OCBC Business mobile: klik "**Masuk → Blokir User Saya**" dan ikuti instruksi yang tertera pada layar.

   [EN] If your device or mobile number is stolen or lost, or is suspected of being misused by another party, take the following steps.
   a. Block your Software Token
      You can send an email request to clientservices@ocbc.id using the email address registered in the OCBC Business system. Please provide your Organization ID, User ID, and Token type, i.e. Software Token.
   b. Block User Access
      - OCBC Business web: click "**Block My User**" on the OCBC Business web login page (https://business.ocbc.id) and follow the on-screen instructions.
      - OCBC Business mobile: select "**Log in → Block My User**" and follow the on-screen instructions.

   [CN] 如果您的设备或手机号码被盗、遗失或疑似被他人滥用，请采取以下措施。
   a. 停用您的 Software Token
      您可以使用在 OCBC Business 系统中登记的电子邮箱发送申请至 clientservices@ocbc.id。请提供您的 Organization ID、User ID 以及 Token 类型，即 Software Token。
   b. 停用用户访问权限
      - OCBC Business 网页版：在 OCBC Business 网页登录页面 (https://business.ocbc.id) 点击"阻止我的用户"，并按照屏幕上的指示操作。
      - OCBC Business mobile：点击"**Log in → 阻止我的用户**"，并按照屏幕上的指示操作

Penipuan Daring (Phishing) | Phishing | 网络钓鱼

[ID] 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 email, pesan instan, telepon, SMS, dan lain-lain.

[EN] Phishing is a fraudulent attempt in the cyber world to unlawfully obtain personal information such as User ID, Password, PIN, and account number. Phishing is commonly carried out through electronic communication channels such as email, instant messages, phone calls, SMS, and others.

[CN] 网络钓鱼 (Phishing) 是一种网络诈骗行为，旨在非法获取个人信息，例如 User ID、密码、PIN 或账户号码。网络钓鱼可通过电子邮件、即时通讯、电话、短信等各种电子通信渠道进行。

Beberapa teknik penipuan phishing yang biasa dilakukan | Several phishing techniques that are commonly used | 常见的网络钓鱼手法包括：

1. **[ID]** Menggunakan alamat email palsu untuk meminta informasi rahasia dengan berbagai alasan, misalnya perbaikan sistem maupun upgrade.

   [EN] Using a fake email address to request confidential information for various reasons, such as system repairs or upgrades.

   [CN] 使用虚假电子邮箱地址，以系统维修、升级等各种理由要求您提供机密信息。

2. **[ID]** 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.

   [EN] Using a fake website that resembles the official website. Phishing perpetrators may create a fake website with the same or similar name but use a different domain, or alter one or two letters in the URL.

   [CN] 使用与官方网站相似的虚假网站。网络钓鱼者通常会创建名称相同或相似的虚假网站，但使用不同的域名，或仅更改网址 (URL) 中的一两个字母。

3. **[ID]** Mengirimkan form isian melalui email, SMS, aplikasi chatting online, atau menghubungi melalui telepon dengan mengaku sebagai pihak Bank untuk meminta informasi ID Pengguna, Kata Sandi, atau PIN.

   [EN] Sending forms via email, SMS, online messaging applications, or contacting you by phone while impersonating a Bank representative to request your User ID, Password, or PIN.

   [CN] 通过电子邮件、短信、在线聊天应用程序发送表格，或通过电话冒充银行人员，要求您提供 User ID、密码或 PIN。

4. **[ID]** Mengirimkan link yang bertujuan untuk mengarahkan ke suatu situs web tertentu, yang biasanya merupakan situs web palsu.

   [EN] Sending a link intended to direct you to a particular website, which is typically a fraudulent website.

   [CN] 发送链接将您引导至特定网站，而该网站通常为虚假网站。

Langkah pencegahan phishing | How to prevent phishing | 如何防范网络钓鱼：

1. **[ID]** Pastikan kebenaran identitas alamat pengirim email, SMS, situs web, ataupun media komunikasi lainnya sebelum memberikan respons.

   [EN] Always verify the legitimacy and identity of an email sender, SMS, website address, or other communication media before providing any response.

   [CN] 在作出任何回应之前，请务必核实电子邮件发件人、短信、网站地址或其他通信渠道的身份及真实性。

2. **[ID]** Selalu waspada dan jangan membuka link serta mengisi informasi pribadi Anda jika email atau situs web terlihat mencurigakan.

   [EN] Stay alert and do not click links or provide your personal information if an email or website appears suspicious.

   [CN] 请时刻保持警惕。如果电子邮件或网站看起来可疑，请勿点击其中的链接或填写您的个人信息。

3. **[ID]** Jangan terpancing untuk menyebutkan identitas atau informasi rahasia lainnya jika Anda menerima panggilan dari nomor yang tidak dikenal.

   [EN] Do not disclose your identity or other confidential information if you receive a call from an unknown number.

   [CN] 如果您接到陌生号码的来电，请勿因对方诱导而透露您的身份信息或其他机密信息。

Aplikasi Palsu | Rogue Apps | 虚假应用程序

[ID] 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.

[EN] Rogue apps are illegitimate "look-alike" apps containing malware intended to steal personal/sensitive data or banking credentials. These apps are designed to resemble legitimate mobile banking apps by using the same or similar images and icons and closely imitating the application publisher's name.

[CN] 虚假应用程序是模仿官方应用程序制作的非法应用，其中包含旨在窃取您的个人/敏感数据或银行账户凭证的恶意软件。这类应用程序通常使用与正版应用相同或相似的图片和图标，并模仿应用程序发布者的名称，使其看起来与正版应用相似。

Cara mencegah penggunaan aplikasi palsu | How to prevent downloading rogue mobile banking apps | 如何防范虚假移动银行应用程序：

1. **[ID]** 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.

[EN] Only download the OCBC Business mobile app from the official Apple iOS App Store and Android Google Play Store on your device. The Bank does not authorize the publication or distribution of its applications through other application marketplaces.

[CN] 请仅通过设备上的官方 Apple iOS App Store 和 Android Google Play Store 下载 OCBC Business mobile 应用程序。银行未授权通过其他应用市场发布或提供该应用程序。

2. **[ID]** Sebelum mengunduh aplikasi baru, cek penerbit aplikasi yaitu PT Bank OCBC NISP, Tbk., dan pastikan Anda membaca deskripsi aplikasi secara saksama. Aplikasi palsu biasanya tidak memiliki deskripsi atau memiliki deskripsi yang tidak ada hubungannya dan biasanya memiliki kesalahan penulisan.

   [EN] Before downloading a new app, verify that the application publisher is PT Bank OCBC NISP, Tbk., and carefully read the app description. Rogue apps may have no description, an irrelevant description that does not correspond to the application's functionality, or spelling errors.

   [CN] 下载新应用程序前，请确认应用程序发布者为 PT Bank OCBC NISP, Tbk.，并仔细阅读应用程序描述。虚假应用程序通常可能没有描述、描述内容与应用程序功能无关，或存在拼写错误

3. **[ID]** Pastikan Anda membaca syarat dan ketentuan dengan saksama. Beberapa aplikasi palsu mungkin memiliki syarat dan ketentuan yang terlihat sah.

   [EN] Ensure that you carefully read the terms and conditions. Some rogue apps may contain terms and conditions that appear legitimate.

   [CN] 请仔细阅读相关条款与条件。部分虚假应用程序可能提供看似合法的条款与条件。

4. **[ID]** Aplikasi palsu dapat menguras baterai perangkat Anda dengan cepat, sehingga baterai yang terus-menerus cepat habis dapat menjadi tanda adanya infeksi malware atau virus.

   [EN] Rogue apps may drain your device's battery quickly. A battery that consistently drains unusually fast may indicate a malware or virus infection.

   [CN] 虚假应用程序可能会快速消耗设备电量，因此，如果设备电量持续异常快速下降，可能表明设备已受到恶意软件或病毒感染。

Penipuan Penggantian Kartu SIM (SIM Swap) | SIM Swap | SIM 卡置换诈骗

[ID] SIM Swap adalah modus kejahatan di mana 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 diimplementasikan oleh aplikasi OCBC Business mobile.

[EN] SIM Swap is a fraudulent practice where a fraudster takes over your mobile number by using a false identity to request a new SIM card from your mobile network operator, thereby gaining access to your OTPs and push notifications. This method may compromise the two-factor authentication (2FA) security system implemented in the OCBC Business mobile app.

[CN] SIM 卡置换诈骗是指诈骗者冒用虚假身份向移动通信运营商申请新的 SIM 卡，从而接管您的手机号码，并获取您的 OTP（一次性密码）及推送通知。此类行为可能危及 OCBC Business mobile 应用程序所采用的双重身份验证 [2FA] 安全机制。

Untuk melindungi diri Anda dari SIM Swap | To protect yourself from SIM Swap | 如何防范 SIM 卡置换诈骗：

1. **[ID]** Waspada dengan upaya-upaya phishing dan jangan mengunduh aplikasi palsu di mana pelaku akan memperoleh informasi perbankan dan identitas Anda.

   [EN] Be alert to phishing attempts and avoid downloading rogue apps, through which fraudsters may obtain your banking information and personal identity.

   [CN] 请警惕网络钓鱼行为，并避免下载虚假应用程序，因为诈骗者可能通过这些方式获取您的银行信息及个人身份信息。

2. **[ID]** Daftarkan nomor ponsel Anda untuk push notification untuk selalu memantau transaksi perbankan Anda.

   [EN] Register your mobile number for push notifications to continuously monitor your banking transactions.

   [CN] 请登记您的手机号码以接收推送通知，以便持续监控您的银行交易。

3. **[ID]** 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.

   [EN] If you are unable to receive calls, text messages, or OTPs, immediately contact your mobile network operator for verification and contact the Bank to block banking access associated with your mobile number. This may occur when a fraudster has obtained a new SIM card for your number, causing your existing SIM card to be deactivated.

   [CN] 如果您无法接听电话、接收短信或 OTP，请立即联系您的移动通信运营商进行核实，并联系银行停用与该手机号码关联的银行服务访问权限。这可能是由于诈骗者已成功为您的手机号码取得新的 SIM 卡，从而导致您原有的 SIM 卡被停用。

4. **[ID]** Jangan menonaktifkan/memasang mode silent pada nomor ponsel Anda jika menerima banyak panggilan mengganggu, 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.

   [EN] Do not switch off your phone or set it to silent mode if you receive numerous nuisance calls, as this may be a tactic used by fraudsters to distract you and prevent you from noticing that the mobile network service for your number has been deactivated. Ignore such calls.

   [CN] 如果您收到大量骚扰电话，请勿关闭手机或将手机设置为静音模式，因为这可能是诈骗者用来转移您注意力的手段，使您无法及时察觉手机号码的通信服务已被停用。请忽略此类来电