MUST SAY NO

#Lawantipu2online

Guidebook panduan keamanan digital perbankan

DIGITAL SECURITY

Version 11.2025

DIGITAL SECURITY

DAFTAR ISI

APA ITU DIGITAL SECURITY? MENGAPA PENTING?

Era digital telah menghadirkan berbagai kemudahan, tak terkecuali dalam bidang perbankan. Dengan hadirnya smartphone, kini pengguna dapat melakukan berbagai jenis transaksi perbankan dengan cepat dan praktis, tanpa perlu lagi mengunjungi ATM atau kantor cabang. Terlebih sejak munculnya pandemi, channel digital sudah menjadi pilihan utama untuk menjalankan kebutuhan transaksi pribadi maupun bisnis.

Namun, di balik segala kemudahan tersebut, tersimpan pula masalah keamanan yang mengintai, atau yang dikenal sebagai cyber crime. Ada berbagai celah di transaksi elektronik yang dapat menjadi sumber ancaman keamanan, di antaranya melalui ponsel, SIM card, akun email, dan media sosial. Para penjahat cyber dapat melakukan pencegatan pesan, memonitor panggilan telepon, mencuri informasi pribadi, bahkan menyadap mikrofon ponsel.

OCBC merancang buku panduan ini agar masyarakat mengenali berbagai jenis *cyber crime* yang umum terjadi. Diharapkan, dengan membaca buku ini, masyarakat dapat mengantisipasi dan menghindari jebakan penipuan yang bisa

CONTOH KASUS KEBOCORAN DATA

Kasus kebocoran data bukan merupakan hal baru, dan bisa terjadi di mana saja dalam skala besar maupun kecil. Berikut adalah beberapa contoh kebocoran data yang pernah terjadi:

- Data NIK & dokumen salinan Kartu Keluarga diperjualbelikan oleh pihak-pihak tak bertanggungjawab seharga Rp5.000/data
- Alphabet Incorporated, perusahaan yang menaungi Google, didenda Rp153 miliar dari akumulasi 227 kasus pelanggaran data pribadi penggunanya (CNN Indonesia.com).
- Google dituntut karena skandal WiSpy, yaitu pengambilan data WiFi rumah yang tidak dienskripsi berupa data pribadi penghuninya, dengan menggunakan mobil proyek pemetaan Google Street View.
- Sebanyak 70 pengemudi ojol di Pontianak menerima tagihan sebesar Rp1 juta – Rp23 juta padahal mereka tidak pinjam uang sama sekali. Ternyata, mereka diimingi-imingi uang sebesar Rp100 ribu oleh seseorang untuk memberikan foto KTP dan foto diri. Foto data diri ini digunakan oleh si oknum untuk transaksi Paylater beli tiket jalan-jalan di Traveloka dan membeli gadget.
- Kelalaian Sindikat Data Pinjaman Online dalam menjaga keamanan data nasabahnya, sehingga pihak ketiga bisa dengan mudah melihat data pribadi/basis data.
- Terungkapnya sebuah organisasi di Facebook *[Dream Market Official]* yang memperjual-belikan data pribadi lebih dari 71 ribu orang yang terdaftar di situs *online*, dengan harga Rp350/data.

Penyebab kebocoran data

Bagaimanakah data-data pribadi bisa jatuh ke tangan penipu?

- Pernah mengajukan pinjaman lewat aplikasi online yang tidak resmi atau tidak terverifikasi dan keamanan data tidak terjamin sehingga mudah diretas.
- Pernah memberikan akses, email, file, foto & dokumen melalui aplikasi illegal atau share link kepada orang yang tidak dikenal.
- Kecerobohan perusahaan dalam menyimpan data pribadi karyawan, rincian pembayaran perusahaan yang didapat dari kode otorisasi di *cloud*, folder bersama saat transfer bersama.
- Adanya oknum di instansi pemerintahan, seperti Dukcapil, Dirjen Pajak, dll yang menyalahgunakan data untuk kepentingan bisnis.

MENGAPA ORANG BISA TERTIPU?

Ada beberapa fenomena yang menjelaskan mengapa seseorang dapat menjadi korban penipuan. Kenali penyebabnya agar kamu dapat mengantisipasi dan menghindarinya.

OPTIMISM BIAS

Kecenderungan berpikir terlalu positif dan mengabaikan risiko yang menyebabkan seseorang meyakini bahwa ia berisiko lebih rendah dibandingkan dengan orang lain untuk tertimpa hal negatif (misalnya : terkena penipuan)

PRINSIP PERSUASIF

Dengan menggunakan prinsip persuasif, orang yang berniat jahat bisa memanipulasi seseorang sehingga bertindak sesuai dengan apa yang ia harapkan.

KREDIBILITAS

Menggunakan otoritas/ mengatasnamakan dari instansi tertentu.

Contoh:
Saya dari pegawai bank A ingin menginfokan untuk melakukan pengkinian data dengan klik link web.xxx sekarang.

NORMA BERLAKU

Menciptakan rasa urgensi.

Contoh:
Penipu menghubungi dan mengatakan kebijakan peningkatan biaya admin yang akan segera berlaku. Jika Anda ingin menolak kewajiban mengisi formulir pada pesan ini.

TIMBAL BALIK

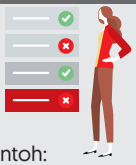
Korban merasa memiliki 'hutang' kepada pelaku, sehingga lebih mudah dimanipulasi.

Contoh:
Pemberian hadiah palsu seperti penawaran investasi menarik atau tawaran bantuan bantuan yang sebenarnya tidak ada.

KELANGKAAN

Sesuatu menjadi lebih diinginkan ketika stock terbatas.

Contoh:
Segera dapatkan hadiah iPhone 17 dengan klik link web.xxx ini! Hadiah terbatas klik sekarang juga.n



KOMITMEN

Membujuk korban agar memberikan bantuan atau uang, meskipun awalnya ragu.

Contoh:
Penipu meyakinkan korban untuk melakukan investasi kecil dengan janji keuntungan besar. Lalu dibujuk untuk melakukan investasi dengan nominal yang lebih besar.

HUBUNGAN

Menggunakan jalinan hubungan sebagai alasan untuk menolong si penipu.

Contoh :
Berpura-pura menjadi teman seperti "Halo bisa minta tolong urgent pinjam Rp1 Juta dulu nanti segera kembalikan".

MENGAPA ORANG BISA TERTIPU?

Berhati-hatilah karena penipu bisa berpura-pura menjadi orang yang sangat mengenal Anda seperti keluarga, teman dekat, rekan kerja atau bisa juga memposisikan diri sebagai petugas bank ataupun instansi pemerintah yang Anda percayai

AREA INTERVENSI

Apa saja data pribadi yang menjadi sumber informasi kejahatan?

- Alamat lengkap
- No. ponsel
- Emergency contact/kerabat
- Foto selfie
- Nama ibu kandung
- No. rekening dan slip gaji
- Kartu Keluarga
- KTP
- Limit kartu kredit

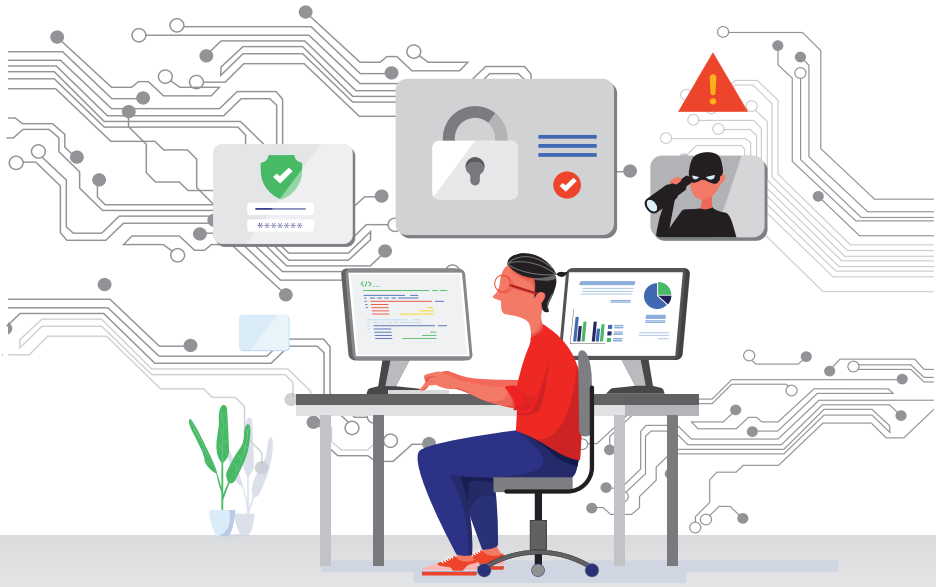
Data-data tersebut bisa disalahgunakan untuk pengajuan pinjaman online, aksi terorisme, ataupun jual beli narkoba.

Penting! Pihak Bank OCBC tidak pernah meminta informasi-informasi dibawah ini dengan alasan apapun melalui SMS, Email, maupuan telepon:

- PIN
- OTP
- User ID
- Password
- CVV Kartu Kredit/Debit

APA YANG HARUS DILAKUKAN UNTUK MENGHINDARI CYBER CRIME?

- Hati-hati memberikan data pribadi kepada pihak mana pun
- Jangan memberikan data secara berlebihan dan tidak relevan. Kritislah terhadap permintaan akses pada aplikasi di ponsel, terutama jika sebuah aplikasi meminta akses ke data kontak, galeri foto, dan lokasi melalui GPS.
- Jangan sembarangan login ke situs yang tidak-tidak, misalnya situs kencan online, dengan alamat email yang terhubung dengan email perbankan kamu.
- Bersihkan file digital di ponsel secara rutin.
- Jangan unggah/scan foto pribadi karena bisa dipakai untuk memberikan otorisasi.
- Jangan unggah tiket perjalanan ke media sosial, karena itu berarti mengumumkan kapan kamu tidak berada di rumah, sehingga memudahkan orang yang berniat jahat.
- Perusahaan perlu menumbuhkan budaya peduli bisnis dan keamanan.
- Gunakan password yang rumit dan tidak mudah ditebak.
- Jangan memberikan tanda tangan pada kuitansi kosong untuk mengambil kredit pinjaman, pastikan data terisi lengkap baru ditanda tangan.

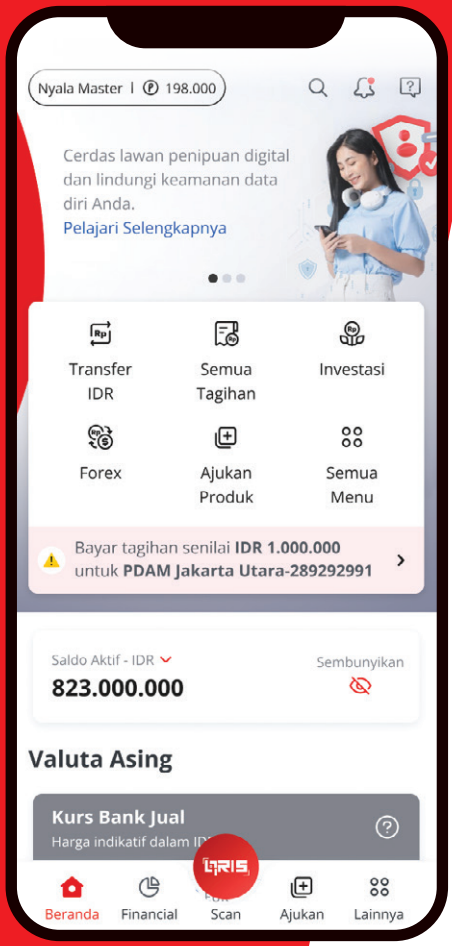


Tips & trik bertransaksi aman di digital

A. Bertransaksi melalui OCBC mobile

Saat ini, hampir semua transaksi perbankan dilakukan melalui aplikasi mobile banking di smartphone. Tentunya, perangkat ini menjadi incaran para penjahat digital untuk bisa masuk ke akun mobile banking dan menguras uang yang ada di rekeningmu.

OCBC memiliki OCBC mobile sebagai aplikasi digital perbankan yang merupakan *one stop digital solutions for all your banking needs*. Penting sekali untuk memastikan keamanan secara berlapis setiap bertransaksi di OCBC mobile, agar kamu bisa bertransaksi dengan lancar dan aman.



PERBEDAAN PASSWORD DENGAN PIN TRANSAKSI

Saat bertransaksi melalui *channel online*, diwajibkan untuk menerapkan Two-Factor Authentication (2FA) atau verifikasi dua langkah, yang berfungsi untuk lebih mengamankan akunmu dari berbagai kejahatan digital.

OCBC mobile menerapkan 2FA ini dengan dua jenis fitur keamanan, yaitu password dan PIN Transaksi.

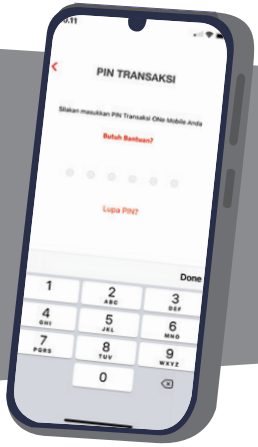
Apakah perbedaan dari kedua istilah tersebut?

Password

Kata sandi atau password digunakan untuk untuk login ke dalam *online banking* (OCBC mobile atau Internet Banking).
Sebagai alternatif *password*, nasabah bisa mengaktifkan *Finger Print/Face ID* untuk *login* ke OCBC mobile.

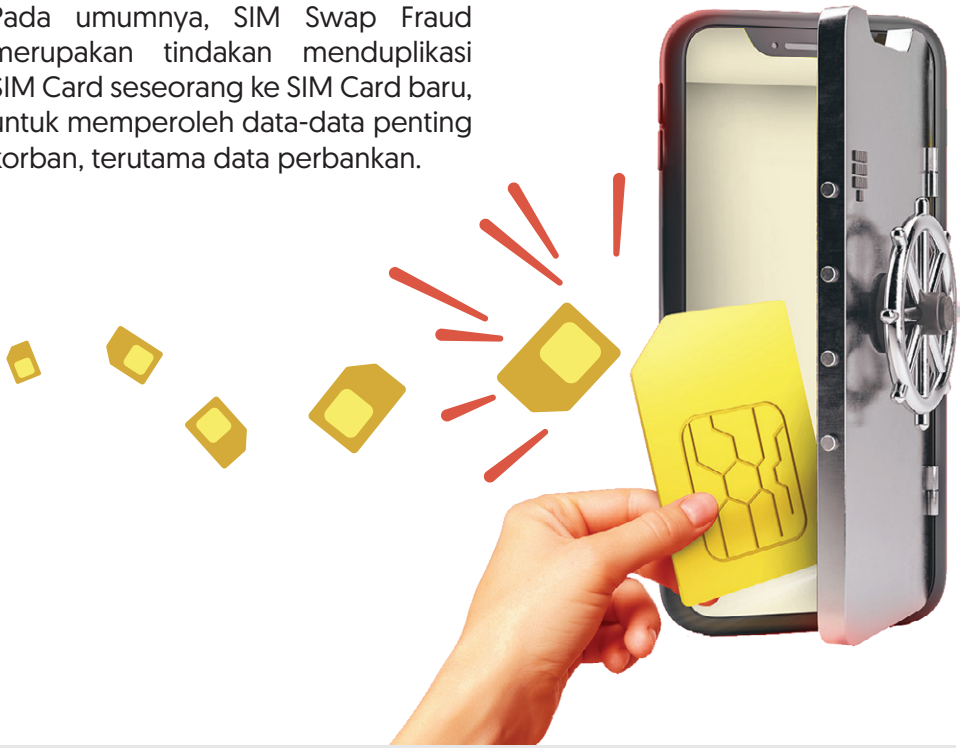
PIN Transaksi

PIN Transaksi digunakan untuk melakukan otorisasi transaksi. Apabila lupa, PIN Transaksi bisa di aktifkan ulang (selama belum terblokir) melalui menu Pengaturan.



SIM SWAP FRAUD

Pada umumnya, SIM Swap Fraud merupakan tindakan menduplikasi SIM Card seseorang ke SIM Card baru, untuk memperoleh data-data penting korban, terutama data perbankan.



Cara-cara untuk menghindari SIM SWAP:

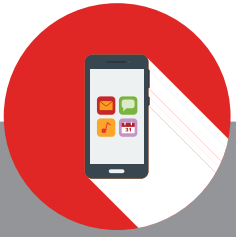
1. Waspada apabila ada telepon/SMS permintaan untuk mematikan ponsel sementara, mengetikan suatu kode khusus di ponsel Anda, atau menanyakan data-data pribadi Anda.
2. Segera hubungi operator seluler Anda apabila layanan komunikasi ponsel tiba-tiba tidak berfungsi, seperti tidak dapat melakukan/menerima panggilan atau SMS.
3. Jangan mempublikasikan nomor ponsel Anda di media sosial, atau gunakan nomor yang berbeda untuk aktivitas perbankan.
4. Lindungi data-data pribadi perbankan Anda, seperti User ID, kata sandi, PIN, OTP, dan informasi lainnya.
5. Selalu pantau transaksi finansial dalam rekening Anda melalui OCBC mobile.

DEVICE SECURITY

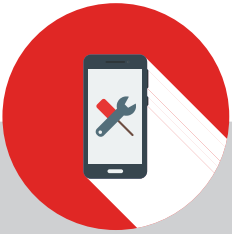
Perangkat seluler membuat hidup jauh lebih nyaman, karena kamu dapat bertransaksi perbankan kapan dan di mana saja cukup dengan aplikasi mobile banking. Namun, smartphone juga dapat melacak identitas kamu, lokasi di mana kamu berada, dan informasi tentang teman, keluarga, dan kontak kamu. Hal ini dapat membuat kamu dan perangkatmu menjadi target utama peretas.

Pasang kata sandi/keamanan tambahan pada ponsel.

Sebagai langkah awal kemanan, lindungi ponsel dengan menggunakan kata sandi/PIN 6 angka ataupun menggunakan biomatric (Finger Print/Face ID). Hindari menggunakan kata sandi yang mudah ditebak.



Cek kembali semua aplikasi yang ada di ponsel kamu. Pastikan aman & diunduh dari store resmi. Hindari mengunduh aplikasi perbankan dari web ataupun link yang tidak resmi.



Hindari menggunakan perangkat yang sudah di-jailbreak atau rooted.

B. Keamanan berbelanja *offline & online*

Berbelanja kebutuhan sehari-hari, baik di toko, supermarket atau mall, tak bisa dipisahkan dari kehidupan masyarakat. Selain itu, dalam beberapa tahun belakangan, kita juga telah merasakan kemudahan bertransaksi secara online melalui *platform* digital *e-commerce*. Pembayaran non-tunai pun semakin populer karena dinilai lebih praktis dan aman. Namun ternyata sistem ini tidak sepenuhnya aman, karena penjahat digital masih saja bisa menjalankan aksi penipuan melalui berbagai alat pembayaran yang kita gunakan.

KERAHASIAAN OTP

Kode OTP *(One Time Password)* adalah Kode Rahasia yang akan kamu dapatkan saat melakukan pembayaran belanja *online*.

Cara-cara untuk menghindari Kebocoran Rahasia OTP:

Jaga kerahasiaan Kode OTP kamu dan jangan pernah informasikan kode ini kepada siapa pun, termasuk Petugas Bank.

KEAMANAN KARTU KREDIT

Apabila kita tidak berhati-hati menggunakannya, kartu kredit rentan disalahgunakan oleh pelaku tindak kejahatan sebagai alat pembayaran yang tidak sah. Umumnya, modus dari kejahatan ini adalah berkedok pengajuan KTA Online, atau bisa juga menggunakan alat penduplikasi data seperti mesin gesek yang digunakan sebagai pembayaran kartu kredit. Dengan alasan untuk keperluan administrasi, seringkali instansi tertentu mensyaratkan fotokopi KTP atau dokumen-dokumen lainnya. Demi keamanan, jangan pernah melakukan duplikasi kartu kredit dengan cara fotokopi. Orang masih bisa menyalahgunakan kartu kreditmu meski hanya melalui fotokopi. Selain itu, harap selalu diingat bahwa bank tidak pernah meminta fotokopi kartu kredit sebagai dokumen persyaratan.

Agar terhindar dari penyalahgunaan kartu kredit:

1. **Jaga kerahasiaan identitas pribadi**
   Jangan berikan informasi pribadi seputar kartu kredit kamu kepada pihak-pihak yang tidak berkepentingan. Misalnya nama gadis ibu kandung, masa berlaku kartu kredit, limit kartu, apalagi tiga digit di bagian belakang kartu yang sering disebut CVV (Card Verification Value).

2. **Gunakan PIN dalam bertransaksi**
   Efektif per 1 Juli 2020, seluruh transaksi kartu kredit wajib menggunakan PIN 6 Digit. Gunakan PIN dengan kombinasi angka yang mudah diingat, namun sedapat mungkin hindari penggunaan tanggal lahir pribadi, anak atau pasangan sebagai nomor PIN karena mudah ditebak.

3. **Aktifkan notifikasi transaksi**
   Aturlah agar kamu menerima SMS notifikasi secara otomatis untuk setiap transaksi menggunakan kartu kredit. Apabila mendapat notifikasi padahal tidak merasa bertransaksi, segera laporkan kepada bank penerbit kartu.

4. **Pastikan kartu kreditmu selalu dalam pengawasanmu**
   Simpan dan jagalah kartu kredit dengan baik, jangan sampai kartu kreditmu berpindah tangan dengan sembarangan. Awasi baik-baik setiap transaksi yang dilakukan di restoran, tempat belanja, dan tempat lainnya.

5. **Langsung laporkan ke pihak penerbit apabila terjadi kehilangan**
   Laporkan kepada bank atau penerbit begitu kamu menyadari kartu kredit kamu hilang atau dicuri. Lakukan pemblokiran segera mungkin untuk mencegah pencurian identitas atau keharusan membayar tagihan yang tidak semestinya.

DIGITAL SECURITY

KEAMANAN KARTU DEBIT

Ada berbagai macam ragam tindak kejahatan penyalahgunaan kartu debit sebagai alat pembayaran yang tidak sah. Salah satu modus pencurian yang paling umum adalah aksi skimming. Pelaku kejahatan mendapatkan dan menyalin informasi data nasabah yang terdapat pada strip kartu debit (bagian belakang kartu debit yang biasanya berwarna hitam). Aksi ini dapat terjadi saat nasabah menggunakan layanan ATM.

Agar terhindar dari kejahatan kartu debit:

1. ***Chip Based Security***
   Pastikan kartu debit kamu sudah menggunakan teknologi chip yang lebih aman. Jika kamu masih menggunakan kartu debit lama yang berteknologi magnetic, segera tukarkan ke cabang terdekat.

2. **PIN Debit 6 Digit**
   - Pastikan kamu menggunakan PIN 6 Digit setiap bertransaksi belanja dengan kartu debit.
   - Ubah PIN tersebut secara berkala.
   - Hindari angka PIN 6 digit yang berhubungan dengan kamu secara langsung, misalnya tanggal lahir pribadi anak atau pasangan.

3. **Pastikan kartu debitmu selalu dalam pengawasanmu**
   Simpan dan jagalah kartu debit dengan baik, jangan sampai kartu debitmu berpindah tangan dengan sembarangan.

4. **Langsung laporkan ke pihak penerbit bila terjadi kehilangan**
   Laporkan kepada bank atau penerbit begitu kamu menyadari kartu debit kamu hilang atau dicuri. Lakukan pemblokiran sesegera mungkin untuk mencegah pencurian identitas atau keharusan membayar tagihan yang tidak semestinya.

DIGITAL SECURITY

KEAMANAN KARTU DEBIT VIRTUAL

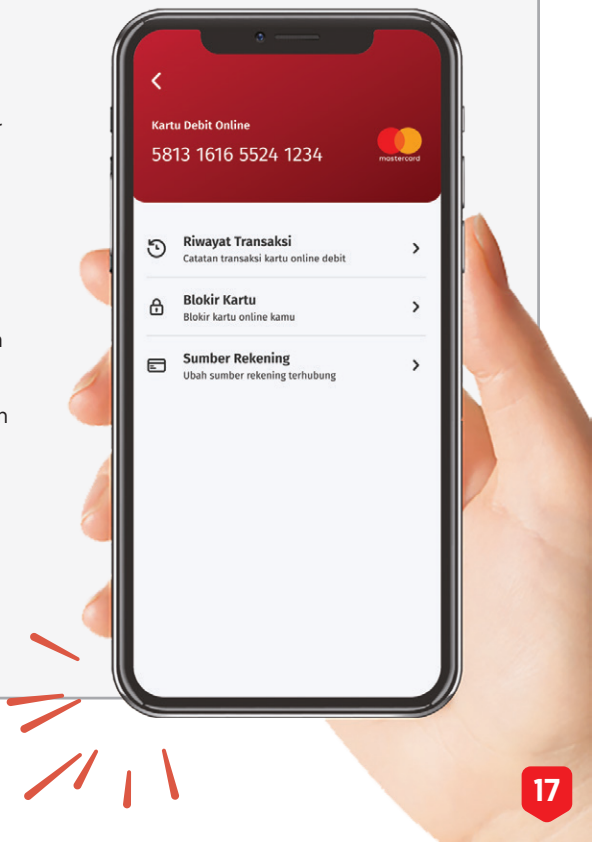
Kartu debit virtual adalah alat transaksi serupa kartu kredit atau debit yang dilengkapi dengan nomor kartu, tiga angka CVV (Card Verification Value) dan tanggal kedaluwarsa *(expiration date)*.

Umumnya, kartu debit virtual digunakan untuk bertransaksi secara online di e-commerce atau aplikasi penyedia layanan hiburan berlangganan seperti Netflix, Spotify, dan sebagainya.

Bagi Nasabah OCBC, kartu debit virtual dapat dibuat & digunakan melalui aplikasi OCBC mobile.

Agar kartu debit virtual tidak disalahgunakan:

1. Jaga kerahasiaan data pribadi
   Jangan berikan informasi seputar data pribadi, seperti User ID, Password Online Banking, No. HP, dan lainnya kepada siapa pun. Umumnya, kartu debit virtual diakses melalui aplikasi mobile banking, jadi pastikan informasi untuk mengaksesnya terlindungi dengan baik.
2. Manfaatkan fitur keamanan kartu debit virtual
   Beberapa kartu debit virtual memiliki fitur untuk meningkatkan keamanan. Melalui aplikasi OCBC mobile, kamu bisa mengatur limit transaksi dengan kartu debit virtual, sehingga mengurangi risiko penggunaan dengan jumlah besar.
3. Lakukan transaksi di e-commerce/situs yang terpercaya
   Saldo kartu debit virtual terhubung dengan tabungan, sehingga akan langsung memotong saldo rekening. Agar menjamin transaksi yang kamu lakukan aman, pastikan hanya bertransaksi pada e-commerce, aplikasi, atau situs yang terpercaya.
4. Blokir segera apabila ada transaksi yang mencurigakan
   Apabila kamu menerima notifikasi atas transaksi yang mencurigakan, segera lakukan pemblokiran kartu debit virtualmu.



DIGITAL SECURITY

KEAMANAN QRIS

Melalui menu QRIS di OCBC mobile , kamu dapat melakukan pembayaran secara non-tunai di semua merchant yang sudah menerapkan standar QRIS.

Pembayaran menggunakan QRIS sangat mudah, namun kamu tetap harus memperhatikan keamanan saat bertransaksi untuk menghindari hal-hal yang tak diinginkan.

Agar bertransaksi QR semakin aman:

1. Lindungi User ID dan Password mobile banking
   Penggunaan QRIS mungkin dilakukan di area umum. Pastikan kamu melindungi informasi password mobile banking dari orang di sekitar kamu. Akan lebih aman apabila kamu mengaktifkan Fingerprint/Face ID untuk login ke mobile banking.
2. Cek detail transaksi sebelum melakukan pembayaran
   Transaksi menggunakan QR sangat mudah & cepat, namun ada baiknya untuk melakukan pengecekan lebih detail sebelum menyetujui transaksi. Jangan sampai QR Code yang dipindai bukan yang seharusnya.
3. Waspadai QR code yang dipindai
   QR code memang sulit dibedakan yang asli atau yang palsu. Maka, ada baiknya lebih waspada apabila ketika memindai QR code yang otomatis mengunjungi situs web tertentu, karena bisa saja situs yang dikunjungi sudah dipersiapkan untuk mengeksploitasi data pribadi atau mengandung virus.

E-COMMERCE SECURITY

Waspadai tanda-tanda yang mencurigakan dari *e-commerce*. Semakin banyak tanda mencurigakan, semakin besar kemungkinan penipuan.

Gadget terbaru dengan harga sangat miring!

Pembayaran harus dilakukan di muka!

Pembayaran hanya melalui Bank Transfer!

Tidak bisa bertemu langsung!

Penipu bisa saja memberikan jaminan sebagai bagian dari usaha mereka untuk mendapatkan kepercayaan kamu. Biasanya jaminan tersebut sulit dilacak kebenarannya.

Ini foto identitas saya dan alamat saya di ...

Jangan khawatir, akun bank saya dari bank lokal

Barang bisa di-*refund* (uang dikembalikan)

Anda punya nomor telepon saya! Jangan khawatir!

Cara supaya akun e-commerce kamu aman dari cyber crime

- Melakukan transaksi di dalam platform dan hanya gunakan pilihan pembayaran yang aman.

- Hindari pembayaran di muka. Jika memungkinkan, lakukan pembayaran saat barang sudah diterima.

- Lihat kredibilitas penjual.

C. Penipuan pinjaman yang mengatasnamakan bank

Banyak penipuan dengan iming-iming pinjaman uang, dan pelakunya adalah orang yang tidak bertanggung jawab dengan mengatasnamakan Bank. Berhati-hatilah, karena:

1. Organisasi pemberi pinjaman resmi tidak akan meminta pembayaran apa pun sebelum pemberian pinjaman.
2. Jangan pernah ambil resiko untuk memberikan respon kepada mereka.
3. Segera laporkan dan blokir nomor telepon yang diduga melakukan penipuan.

Berhati-hatilah selalu jika dihubungi nomor ponsel yang tak dikenal, untuk melindungi diri kamu dari cyber crime.

Jasa Pinjaman Online yang Aman

1. Pastikan terdaftar di OJK.
2. Baca dan pahami baik-baik seluruh Syarat & Ketentuan yang ada.
3. Waspada dengan permintaan akses data di ponsel seperti kontak, galeri foto, dan izin publikasi data.

Kita harus teliti di awal, pahami risiko bahwa data dapat langsung diakses untuk tindak kejahatan

PENIPUAN DENGAN MENIRUKAN EMAIL

Saat ini, email menjadi hal yang wajib dimiliki, tidak hanya untuk keperluan mengirim/menerima pesan tetapi juga berguna sebagai penghubung dengan berbagai aplikasi penting, misalnya yang berhubungan dengan perbankan. Itu sebabnya, email menjadi sasaran utama para hacker atau orang yang tidak bertanggung jawab untuk mencuri data penting, termasuk dalam urusan pekerjaan dan bisnis.

Berikut modus penipu meretas email kamu:

Meretas akun email dan memonitor email tersebut

Bertindak seperti supplier atau boss

Mengirim email penipuan yang meminta sejumlah pembayaran ke akun bank baru

Penipu bisa saja membuat alamat email baru yang mirip dengan alamat email bisnis resmi.

Temukan perbedaannya pada contoh tabel berikut:

ACTUAL	EMAIL TIPUAN
lisa@gmail.com	1isa@9mail.com
payment@appleintl.com	payment@appleIntl.com
finance@deshipping.com	finance@deshpping.com
theboss@gmail.com	theboss@qmail.com
abc@de.international.com	abc@de-international.com

PENIPUAN DENGAN MENIRUKAN EMAIL

Beberapa cara mudah untuk menjaga keamanan informasi email:

- Berjaga-jaga untuk setiap perubahan mendadak yang berkaitan tentang instruksi pembayaran atau permintaan tidak biasa yang mengatasnamakan atasan kamu, partner bisnis, atau kreditur.

- Selalu cek kebenaran dari suatu permintaan/perubahan dengan cara menghubungi pihak lain menggunakan nomor kontak yang telah diketahui sebelumnya, daripada menggunakan informasi pada *email*.

- Gunakan password yang kuat sehingga tidak mudah ditebak. Ganti password secara berkala dan gunakan *Two-Factor Authentication* (2FA).

- Lakukan pengecekan virus di komputer kamu secara rutin.

- Pasang aplikasi anti-virus, *anti-spyware/malware*, dan *firewall* di komputer kamu, dan pastikan aplikasi tersebut terus ter-*update*.

- Hindari menggunakan *software*/aplikasi bajakan.

- Berikan edukasi kepada karyawan berkaitan dengan jenis penipuan ini, khususnya untuk mereka yang bertanggung jawab dalam melakukan pembayaran.

- Waspada dengan dengan *social engineering* yang dilakukan melalui *email*.

VOICE PHISING SCAMS

Voice phishing (vishing) adalah bentuk penipuan melalui telepon, dengan tujuan memancing korban agar memberikan informasi pribadi yang bersifat personal dan sensitif. Dalam menjalankan aksi vishing, si penipu menciptakan skenario yang menyerang emosi targetnya dan meyakinkan korban untuk mengungkapkan informasi sensitif, seperti nomor kartu kredit, kata sandi, atau detail pribadi lainnya yang dapat digunakan untuk mengakses rekening bank target, atau dengan menipu target agar mentransfer uang secara langsung. Aksi ini lebih banyak menargetkan orang tua atau orang yang kurang paham teknologi, yang tidak familiar dengan jenis penipuan ini.

Salah satu jenis vishing lainnya adalah serangan pada rekening bank. Pelaku akan mengincar akses informasi ke akun bank dan jika sudah memiliki akses ke data pribadi, mereka dapat dengan mudah berpura-pura menjadi bank tertentu dan memulai aksi penipuan kepada para nasabahnya. Misalnya, "bank" menawarkan untuk mengirim kartu ATM baru dan meminta target memasukkan PIN. Jika target benar melakukannya maka para vishers akan dapat menduplikasi kartunya dan menggunakannya secara bebas.

Bagaimana cara mencegah *vishing*?

- Ketika menerima telepon yang mengatasnamakan bank, pastikan dulu apakah penelepon benar-benar dari pihak bank atau bukan. Tidak ada salahnya kamu menutup telepon dulu dan kemudian menelepon balik. Dalam kasus *vishing*, pelakunya tidak akan mengangkat panggilan tersebut.
- Kamu harus curiga jika ditelepon atas nama bank yang meminta kamu menjawab terkait data pribadi seperti PIN ATM, karena pihak bank tidak mungkin menanyakan hal tersebut. Jangan berikan data pribadi untuk transaksi perbankan kepada siapapun, termasuk petugas bank.
- Jangan panik saat kamu menjadi calon korban dari tindak penipuan *vishing (voice phishing)*. Berpikirlah dengan jernih sehingga kamu bisa tahu apa yang harus dilakukan.

Intinya, *vishing* adalah tindakan penipuan via telepon yang bertujuan menciptakan rasa urgensi yang salah, membuat target berpikir bahwa mereka dalam kesulitan, atau justru mendapat kesempatan emas dan perlu bertindak sesegera mungkin agar tidak kehilangan kesempatan itu. Maka, tidak ada salahnya untuk menutup telepon sejenak, cari informasi tentang penelepon dengan memasukkan nomor telepon tersebut di pencarian internet, dan kemudian menelepon kembali setelah melakukan riset singkat tadi.

SMS PHISING

Smishing, atau *SMS phishing*, adalah tindakan melakukan penipuan melalui media pesan teks dengan cara mencoba mempengaruhi target untuk mengungkapkan informasi pribadi mereka atau menginstal malware pada perangkat, yang selanjutnya akan disalahgunakan untuk tindak kriminal.

Bagaimana cara melindungi diri dari *SMS phishing*?

- Waspadai SMS mencurigakan yang mengaku dari pihak bank dan meminta kamu untuk mengungkapkan data yang bersifat rahasia seperti PIN/OTP. Langsung hubungi pihak bank yang bersangkutan melalui nomor resmi.
- Tetap waspada sebelum meng-klik link apa pun yang ada di dalam SMS.
- Berhati-hatilah untuk tidak mengungkapkan data pribadi maupun data yang tercatat di pihak bank kepada siapapun, seperti nomor ATM/Kartu Debit/Kartu Kredit, PIN, akses menuju *online banking*, dan OTP yang tersambung ke aplikasi.
- Selalu mengetik URL secara langsung di *browser* untuk mengurangi risiko penipuan.
- Selalu membaca setiap SMS dengan benar dan teliti dari ponsel kamu terkait transaksi yang dilakukan.
- Segera hubungi pihak bank saat ada perubahan detail kontak seperti nomor telepon atau alamat email, sehingga kamu bisa tetap menerima SMS atau notifikasi email terkait aktivitas dan transaksi di *online banking*.
- Jangan pernah mengirim uang kepada siapapun yang tidak kamu kenal.

MEDIA SOSIAL & WEBSITE RESMI

Menggunakan media sosial memang sangat menyenangkan, namun tanpa sadar kamu telah membagikan informasi tentang teman, keluarga, dan kontak kamu yang bisa dilihat siapa saja. Informasi yang kamu cantumkan dapat digunakan oleh penipu sebagai bagian dari upaya rekayasa sosial.

Beberapa cara untuk membantu kamu menjaga keamanan informasi media sosial, termasuk akun e-commerce:

- Batasi informasi pribadi yang kamu publikasikan di sosial media, seperti nama anak, nama sekolah, nama hewan peliharaan, dll) karena informasi pada profil utama kamu dapat menjadi jawaban dari pertanyaan yang digunakan untuk otentikasi data pribadimu.

- Laporkan aktivitas mencurigakan atau spam ke situs media sosial yang digunakan untuk mengontak kamu. Spam dapat muncul dalam bentuk posting, pesan, email, atau permintaan pertemanan.

- Ganti kata sandi/password kamu secara berkala dan laporkan aktivitas mencurigakan jika kamu merasa seseorang telah mengakses akun media social.

- Jika kamu yakin sedang menjadi target di platform media sosial apa pun, segera laporkan media sosial tersebut. Facebook, LinkedIn, X, Snapchat dan Instagram memberikan instruksi spesifik tentang cara melakukannya.

- Menemukan akun palsu yang pakai fotomu? Jangan dibiarkan saja, segera laporkan!

PENIPUAN LEWAT MEDIA SOSIAL/ SITUS TIDAK RESMI OCBC NISP

Awas! Hati-hati dengan akun media sosial palsu yang mengatasnamakan OCBC.

Beberapa waktu lalu, kami mendapatkan laporan dari followers dan nasabah terkait tindakan penipuan oleh akun-akun penipuan (fraudster) ini. Mereka menanyakan data pribadi seperti User ID One Mobile, kode CVV, nama ibu kandung, ataupun tempat/tanggal lahir kepada nasabah melalui Direct Message di media sosial.

Kami telah melakukan tindakan mitigasi dengan melaporkan akun-akun fraudster kepada pihak terkait, dan saat ini akun-akun tersebut sudah ditutup dan dihapus. Hal ini kami lakukan untuk melindungi dan menjaga kepercayaan nasabah.

Oleh karena itu, dukung kami dalam gerakan MUST SAY NO & #LawanTipu2Online dengan melaporkan akun-akun palsu mengatasnamakan OCBC yang kalian temukan kepada kami melalui Contact Center, dan follow akun resmi OCBC yang memiliki centang biru.

Akun & nomor OCBC resmi

tanya@ocbc.id atau *email* resmi OCBC lainnya dengan *domain*/akhiran **@ocbc.id**

1500-999 atau +62-21-26506300 (dari luar negeri)

TANYA OCBC: 0812-1500 999
OCBC Indonesia: 0811 2250 0999/ 0811 5850 0999
OCBC Info: 0811 1060 6222

OCBC Info & OCBC CC

ocbc.id atau web.ocbc.id

@ocbc_indonesia

OCBC Indonesia

@OCBC_Indonesia & @Tanya_OCBC

OCBC_Indonesia

ocbc_indonesia

Ocbc Indonesia

D. Login ke Poinseru dengan aman

Poinseru adalah program sekaligus *platform loyalty* yang memberikan *reward* berupa poin untuk setiap transaksi yang dilakukan Nasabah OCBC.

Berhati-hatilah selalu ketika login ke Poinseru menggunakan *User ID* dan *password internet banking/mobile banking*, karena *User ID* dan *password* kamu juga bisa digunakan untuk mengakses rekeningmu.

Tips bertransaksi yang aman dengan Poinseru:

1. Jangan membagikan *User ID Internet Banking/Mobile Banking* maupun *password* ke orang lain bahkan ke petugas bank sekalipun
2. Jangan mencatat *User ID Internet Banking/ Mobile Banking* maupun *password* pada media apapun
3. Selalu *log out* setelah melakukan penukaran poin dan *clear cache* untuk menghilangkan
4. Ubah password dengan mudah lewat OCBC mobile agar keamanan lebih terjaga

MENUKARKAN POINSERU DENGAN AMAN

Kamu bisa menukarkan *(redeem)* Poinseru yang kamu dapatkan dengan hadiah-hadiah berupa *voucher* dan barang.

Untuk menjaga keamanan saat menukarkan Poinseru, kamu perlu melakukan verifikasi *(authentication)* dengan PIN Transaksi di OCBC mobile, lalu memasukkan response code yang ditampilkan di OCBC mobile ke halaman *website* Poinseru.

Tips keamanan saat menukarkan Poinseru:

1. Jangan membagikan kode transaksi PIN OCBC mobile kamu kepada orang lain maupun petugas bank.
2. Jangan mencatat Transaksi PIN OCBC mobile kamu di media apapun.
3. Buat atau ubah Transaksi PIN kamu dengan mudah lewat OCBC mobile agar keamanan lebih terjaga.

E. Tips khusus saat menjelajah internet & mobile

Sebagian besar mesin penjelajah *(browser)* bisa menyimpan data-datamu secara otomatis *(autofill)* seperti kredensial akun, detail kartu bank untuk toko *online*, alamat penagihan, nama, nomor paspor untuk situs perjalanan, dan sebagainya. Jadi, kita tak harus mengisi ulang data yang sama berulang kali. Namun, ternyata hal ini dapat disalahgunakan oleh pelaku kejahatan digital.
Skenario semacam ini menjadi semakin populer di kalangan pelaku kejahatan online. Para pencuri tidak hanya tertarik dengan pengisian data otomatis pada browser; mereka juga bisa mencuri dompet mata uang kripto dan data permainan (gaming), atau file sensitive yang ada di komputermu.
Sebagian besar browser berasumsi bahwa perangkat dan akunmu terlindungi dengan baik, artinya setiap program yang berjalan dari akun di komputer pun bertindak atas pengetahuan kamu dan oleh karenanya harus dapat mengekstraksi dan mendekripsi data yang disimpan. Sayangnya, browser tidak bisa membedakan malware yang telah menembus perangkat dan berjalan di bawah akunmu.

Satu-satunya *browser* yang menawarkan perlindungan ekstra untuk data yang disimpan terhadap pihak ketiga adalah Firefox. *Browser* ini memungkinkan untuk membuat kata sandi utama yang harus kamu masukkan ketika kamu membutuhkan data untuk didekripsi dan digunakan untuk pengisian otomatis. Namun, opsi ini dinonaktifkan secara *default*.

TIPS KHUSUS SAAT MENJELAJAH INTERNET DAN MOBILE

Apa yang Terjadi Pada Data yang Dicuri?

Setelah malware memiliki data autofill dalam bentuk teks biasa, ia akan mengirimnya kembali ke para pelaku kejahatan online. Dari sana, ada dua kemungkinan skenario yang dapat terjadi. Pemilik malware dapat menggunakannya untuk diri sendiri, atau menjualnya ke pihak lain di pasar gelap, di mana produk seperti itu memiliki nilai yang sangat berharga.

Akun yang telah dicuri dapat digunakan untuk banyak tujuan lainnya, mulai dari spamming dan promosi situs web atau aplikasi, hingga pengiriman virus dan pencucian uang yang dicuri dari pihak lain (dan jika polisi terlibat, mereka mungkin akan mengincar jejak kamu).

Bagaimana Melindungi Data dari Para Pencuri

Seperti yang dapat dilihat, jika malware menembus sistem komputermu, data yang tersimpan pada browser bisa berisiko, begitu pula finansial dan reputasi kamu. Untuk menghindari situasi seperti itu, berikut rekomendasi dari Kaspersky:

1. Menjaga Informasi Penting

Jangan mempercayakan informasi penting, seperti detail kartu bank, tersimpan di browser kamu. Masukkan data secara manual setiap kali bertransaksi. Walaupun membutuhkan waktu lebih lama, tetapi jauh lebih aman. Lebih baik lagi, kamu juga dapat menyimpan kata sandi di pengelola kata sandi.

2. Lindungi Data

Jika kamu menggunakan Firefox, kamu dapat melindungi data yang disimpan di browser dengan kata sandi utama. Untuk melakukannya, klik pada tiga bilah di sudut kanan atas browser dan pilih Opsi, buka tab Privasi & Keamanan, gulir ke bawah untuk Login dan Kata Sandi, kemudian pilih kotak Gunakan kata sandi utama (Use a master password box).

Browser akan meminta kamu untuk membuat jenis kata sandi ini. Semakin panjang dan kompleks kata sandi, semakin sulit bagi penyerang untuk memecahkannya.

3. Mencegah Malware Masuk ke Komputer

Paling penting: Cara terbaik untuk melindungi data adalah mencegah malware masuk ke komputer kamu sedari awal. Untuk melakukannya, instal solusi keamanan yang mampu mendeteksi dan mencegah masuknya malware. Tanpa adanya malware, maka tidak akan ada masalah.

"Sumber : wartaekonomi.co.id"

DIGITAL
SECURITY

Ayo MUST SAY NO & #LAWANTIPU2ONLINE Dengan tidak membagikan informasi rahasia kepada siapapun.