TIPS
DATA AMAN
NASABAH NYAMAN
VOL.14

KIAT TRANSAKSI SAAT LIBURAN!
WASPADAI SEGALA BENTUK PENIPUANNYA

Jangan mudah tergiur dengan jenis penawaran apapun juga. Hati-hati, Teliti dan Konfirmasi. Ketiga hal tersebut harus menjadi acuan dalam melakukan setiap transaksi perbankan Anda. Apalagi, menjelang Liburan. Jika tidak, Anda akan tertipu atau perangkap pelaku kejahatan, yang memang sudah mengincar calon korbannya, yang seringkali tidak waspada.

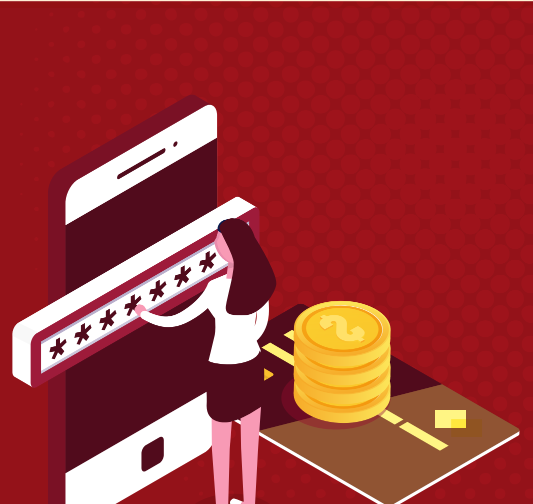
Beralihnya pola transaksi masyarakat umum yang kini lebih menyukai melakukan transaksi secara online, memang membawa sejumlah kemudahan, dengan adanya digital banking, dimana Nasabah dapat melakukan transaksi perbankan, dimana saja. Untuk itu, Bank telah menyiapkan infrastruktur yang didukung dengan sejumlah langkah untuk menjaga keamanan transaksi yang dilakukan Nasabah. Seperti pengiriman One Time Password (OTP) ke handphone Nasabah sebelum terjadinya transaksi untuk mencegah terjadinya penyalahgunaan. Namun perlu disadari bahwa tetap terdapat risiko atas setiap transaksi yang dilakukan.

Beberapa merchant online tertentu telah menyediakan fitur keamanan transaksi dengan meminta Nasabah untuk memasukkan Response Code (Kode Otentikasi Transaksi atau One Time Password disingkat OTP) yang dikirim oleh Bank ke nomor handphone (HP) Nasabah.

Sangat penting, bagi Nasabah untuk waspada terhadap berbagai modus kejahatan yang bertujuan merugikan Nasabah secara finansial, dan untuk itu PermataBank senantiasa memberikan sosialisasi kepada Nasabah untuk menjaga kerahasiaan pengamanan transaksi yang telah ditetapkan oleh PermataBank, yaitu : Personal Identification Number (PIN), Password, User ID, Response Code (Kode Otentikasi Transaksi – One Time Password /OTP), Card Verification Value (CVV) – 3 digit angka terakhir di bagian belakang Kartu Kredit/Debit), juga nomor kartu atau tanggal kadaluarsa kartu (expired date).

Terdapat beberapa modus penipuan yang dilakukan oleh pihak yang tidak bertanggung jawab untuk mendapatkan akses ke rekening Nasabah, diantaranya dengan cara social engineering, dimana pelaku kejahatan melakukan manipulasi psikologis untuk menguak informasi rahasia dari korban yang umumnya dilakukan melalui telepon atau internet. Salah satu cara yang umum dilakukan oleh pelaku kejahatan adalah menawarkan hadiah, namun Nasabah harus menyebutkan kode keamanan perbankannya, misalnya PIN, OTP/kode otorisasi transaksi, CVV dan lainnya. Apabila informasi tersebut dapat diperoleh, maka selanjutnya pelaku kejahatan akan menyalahgunakannya dengan melakukan transaksi pada rekening Nasabah.

Demi keamanan bertransaksi Anda, jagalah kerahasiaan data transaksi tersebut.



One Time Password (OTP) adalah kode verifikasi atau password dinamis yang dikirimkan oleh pihak bank atau situs jual beli online Short Message Services (SMS) atau media lain yang ditentukan oleh bank, untuk meminta persetujuan akses ke rekening nasabah atau memotong pulsa.

Untuk menghindari segala tindakan penipuan yang mengatasnamakan PermataBank, maka Nasabah wajib merahasiakan data/informasi rahasia kartu dan kode OTP yang diterima, serta tidak memberitahukannya kepada siapapun jika tidak merasa melakukan transaksi online.

Nasabah harus memastikan data pribadi pada Bank adalah data terkini, terutama nomor handphone, email atau alamat surat menyurat, untuk memastikan semua informasi terkait transaksi perbankan Anda dapat diterima. Dan pastikan nomor HP yang Anda daftarkan untuk fasilitas OTP adalah nomor HP yang masih dipergunakan.

CONTOH MODUS PENIPUAN

Pelaku menghubungi Nasabah mengatasnamakan diri sebagai petugas dari PermataBank menanyakan beberapa data rahasia seperti data kartu (nomor kartu, expiry date dan CVV) maupun kode OTP yang baru saja terkirim;

Umumnya pelaku memberikan iming-iming seperti penukaran point reward, mendapatkan cashback, mendapatkan undian hadiah mobil/motor, pembatalan transaksi di merchant, pengkinian data Nasabah, konfirmasi perubahan biaya, mendapatkan diskon harga yang tidak masuk akal dan lain-lain.

Korban penipuan dibujuk/ditipu/disyaratkan untuk menyebutkan KODE TERTENTU dari SMS yang diterima korban dengan dalih sebagai kode penukaran atau konfirmasi, namun yang sebenarnya adalah Kode Otentikasi Transaksi (OTP atau Response Code), yang bertujuan untuk MENDEBET DANA Nasabah atas transaksi tertentu.

Kode OTP seringkali diminta dengan dalih sebagai bentuk verifikasi bahwa Nasabah adalah benar orang yang berhak menerima tawaran/iming-iming tersebut;

BERIKUT INI, BEBERAPA TIPS SEBELUM NASABAH MELAKUKAN TRANSAKSI SECARA ONLINE/E-COMMERCE:

✓ TELITI ALAMAT WEBSITE

Sebelum melakukan transaksi, Nasabah harus memastikan keaslian/keabsahan website. Salah satu tanda website yang aman adalah yang diawali dengan "https://", dimana tanda "s" berarti secured (aman). Selain itu, pada bagian bawah browser juga terlihat ikon gembok terkunci.

✓ HINDARI BERTRANSAKSI MELALUI WARNET ATAU HOTSPOT AREA /PUBLIC WIFI.

Lakukan transaksi hanya melalui jaringan yang terpercaya, seperti home wifi yang telah dienkripsi dengan password.

✓ SATU KARTU UNTUK TRANSAKSI ONLINE

Walaupun Nasabah memiliki lebih dari satu kartu, biasakan untuk menggunakan hanya satu kartu tertentu untuk transaksi online.

PENJELASAN SEPUTAR KEJAHATAN E-COMMERCE!

Carding pada e-commerce adalah suatu aktivitas belanja secara on-line (maya, dengan menggunakan data kartu debet atau kartu kredit yang diperoleh secara ilegal).

Kejahatan carding pada e-commerce sangat mudah dilakukan oleh pelaku kejahatan, karena tanpa harus memegang fisik kartu, namun cukup dengan mengetahui informasi tertentu pada kartu debit atau kartu kredit. Antara lain, berupa Card Verification Value (CVV) - berupa 3 digit angka terakhir di bagian belakang kartu kredit/debit), dan masa berlaku pada kartu (expired date), si pelaku sudah dapat melakukan transaksi pada e-commerce.

Beberapa contoh tindakan kejahatan melalui Contact Center palsu.

CONTOH PENIPUAN

1. Dihubungi dengan menggunakan nomor telepon Contact Center palsu
    - Nasabah dihubungi oleh nomor Contact Center palsu, yang mirip dengan PermataTel, yaitu +1500111, menanyakan beberapa data rahasia Nasabah (diantaranya PIN, Password, Response Code (Kode Otentikasi/One Time Password-OTP), User ID, serta Card Verification Value - CVV (3 digit kode pengamanan di belakang Kartu Debit/Kredit).
    - Nomor telepon PermataTel 1500111 tidak pernah digunakan untuk menghubungi Nasabah.

2. Dihubungi dengan email Contact Center palsu.
    - Nasabah mendapatkan email dari alamat email Contact Center palsu, yang mirip dengan care@permatabank.co.id dengan memberikan penawaran atau konfirmasi, dimana Nasabah diminta untuk memberikan beberapa data pribadi Nasabah yang rahasia (PIN, Password, Response Code (Kode Otentikasi/One Time Password-OTP), User ID, serta Card Verification Value (3 digit kode pengamanan di belakang Kartu Debit/Kredit).

3. Memasang stiker yang berisi nomor Contact Center palsu, pada mesin ATM atau ruang ATM.

4. Penipu meminta Nasabah yang menghubungi nomor Contact Center palsu tersebut, dan meminta Nasabah :
    - Menyebutkan data rahasia Nasabah. Seperti PIN, nomor Kartu Kredit, masa berlaku kartu Kredit, atau CVV (3 digit kode pengamanan di belakang kartu Debit/Kredit).
    - Melakukan transaksi di ATM. Seperti : transfer, pembelian atau pembayaran yang menguntungkan pelaku kejahatan, tanpa disadari oleh Nasabah.

PERHATIAN UNTUK KEHATIAN-HATIAN :

1. Tidak menjawab atau memberikan informasi atas pertanyaan sekitar :
    - Personal Identification Number (PIN), Card Verification Value (CVV), One Time Password (OTP) untuk transaksi belanja online, Response Code (kode otentikasi untuk transaksi PermataNet/PermataMobile/SMS Banking), User ID atau Password.
    - Instruksi untuk Nasabah melakukan transaksi, misalnya, transfer atau beli pulsa, di mesin Anjungan Tunaik Mandiri (ATM) atau Internet Banking atau Mobile Banking.

2. Pastikan hanya melihat nomor telepon Contact Center melalui Website (hiperlink dengan website PermataBank), Kartu Debit, Kartu Kredit serta layar dan stiker di ATM.

3. Catat nomor Contact Center pada media lain. Misalnya, di telepon selular (ponsel), atau catatan lainnya, sehingga Nasabah mudah menghubungi Contact Center PermataBank pada saat dibutuhkan.

4. Jangan menyimpan data rahasia seputar rekening atau Kartu Kredit (seperti PIN, CVV), ke dalam perangkat telepon selular (ponsel), laptop, atau komputer

TIPS
WASPADAI SEGALA TINDAK PENIPUAN!

1. Simpan dan perlakukan kartu debet dan/atau kartu kredit dengan baik.

2. Tidak memberikan informasi penting. seperti nomor kartu, tanggal kadaluarsa kartu (expired date), dan Card Verification Value (CVV) – berupa 3 digit angka terakhir di bagian belakang Kartu Kredit/Debit, kepada siapa pun, baik secara langsung maupun media e-mail, website, SMS dan sarana lain.

3. Anda harus menjaga rahasia/data/informasi transaksi, seperti PIN, TIN, Password, User ID, Response Code (Kode Otentikasi Transaksi atau OTP), atau CVV. Semua data tersebut merupakan tanggung jawab Nasabah.

4. Waspadai telepon yang mencurigakan. Segera tutup telepon dan hubungi PermataTel di nomor 1500-111.

5. PermataBank tidak pernah meminta Data Informasi rahasia untuk alasan apa pun juga, Nasabah wajib menjaga kerahasiaannya, dan tidak memberitahukannya kepada pihak lain, termasuk karyawan/petugas PermataBank.

6. Anda harus waspada dan berhati-hati atas segala tindak penipuan, terutama bila ada pihak-pihak yang menghubungi Anda dengan mengatasnamakan PermataBank meminta data rahasia di atas.

7. Menjaga kerahasiaan data, agar tidak terlihat pihak lain saat melakukan transaksi.

8. Jangan mudah tergiur dengan tawaran hadiah atau imbalan yang disampaikan pelaku tertentu, baik melalui telepon atau SMS, yang meminta Nasabah untuk mengirimkan informasi rahasia.

9. PermataBank tidak pernah meminta data/informasi rahasia dari Nasabah, terutama Response Code (Kode Otentikasi Transaksi atau OTP), juga data lainnya seperti password, user ID, PIN atau informasi rahasia lainnya.
   Jangan pernah memberitahukan informasi rahasia kepada orang lain, termasuk petugas PermataBank.

10. Anda wajib menginformasikan kepada Bank, apabila nomor Handphone yang Anda daftarkan untuk fasilitas OTP sudah berubah dan/atau tidak dipergunakan lagi, untuk memastikan agar OTP yang dikirimkan oleh Bank dapat Anda terima.

11. Berbagai Tips dalam menghubungi Contact Center, diantaranya :
    - Hubungi PermataTel di 1500-111.
    - Dari Luar Negeri, Anda dapat menghubungi PermataTel di nomor +6221 2985611.
    - Pastikan Anda mengetahui nomor rekening perbankan atau Kartu Kredit atau Kartu Debit Anda.
    - Pastikan Anda siap dengan data-data yang dibutuhkan untuk verifikasi melalui telepon pada saat Anda menghubungi Contact Center.
    - Sampaikan permasalahan atau pertanyaan Anda kepada staf Contact Center dengan jelas.
    - Pastikan Anda mencatat nomor referensi pengaduan atau pertanyaan Anda.

Jika Anda menemukan hal yang mencurigakan dan tidak wajar, selanjutnya Anda harus menghubungi/konfirmasi PermataBank melalui channel berikut:
(i). PermataTel di nomor 1500-111, atau
(ii). Email : **care@permatabank.co.id**

Kami informasikan pula bahwa kini **Permata**Bank menggunakan teknologi Voice ID yang sangat membantu nasabah dengan memudahkan dan mepercepat proses verifikasi menggunakan pola suara unik dari setiap individu.

Info **www.PermataBank.com** | Permata**Tel 1500111** dengan VOICE ID