Presented by :

PermataBank

TIPS DATA AMAN NASABAH NYAMAN VOL.3

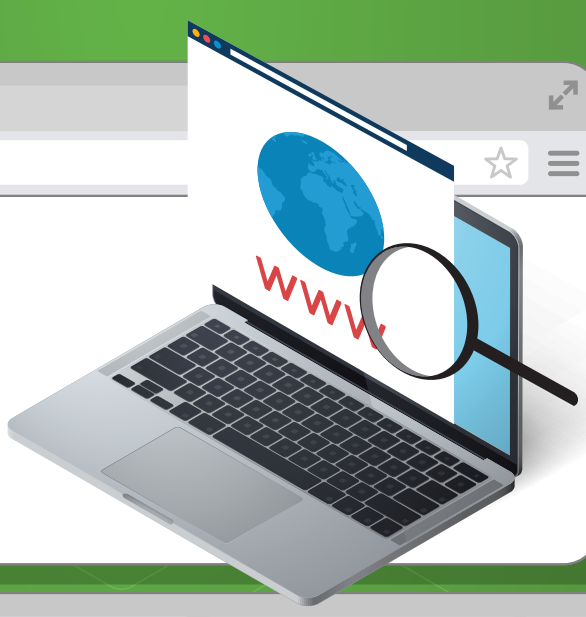
Saat ini banyak terjadi kerawanan bisnis di dunia maya seiring dengan berkembangnya kemudahan bertransaksi melali Digital Banking/Transaksi Online (e-commerce). Seperti potensi peningkatan ancaman kejahatan siber, baik terhadap pedagang, masyarakat sebagai konsumen, bahkan keamanan industri keuangan secara keseluruhan.

Sekarang kejahatan siber yang kerap menerjang transaksi Digital Banking/Transaksi Online (e-commerce) lebih ke perihal menanyakan informasi rahasia untuk proses pembayaran transaksi dengan iming-iming mendapatkan hadiah atau penjualan barang dengan harga murah.

BERIKUT INI, BEBERAPA TIPS SEBELUM NASABAH MELAKUKAN TRANSAKSI SECARA ONLINE:

1). TELITI ALAMAT WEBSITE

Pada saat bertransaksi, Nasabah jangan sampai memasukkan data pribadi di situs palsu. Salah satu tanda website yang aman adalah yang diawali dengan "https://", tanda "s" adalah secured (aman). Selain itu, pada bagian bawah browser juga terlihat ikon gembok terkunci. Jika tidak ada tanda-tanda tersebut, kemungkinan besar Nasabah bertransaksi dalam situs yang tidak aman sama sekali.



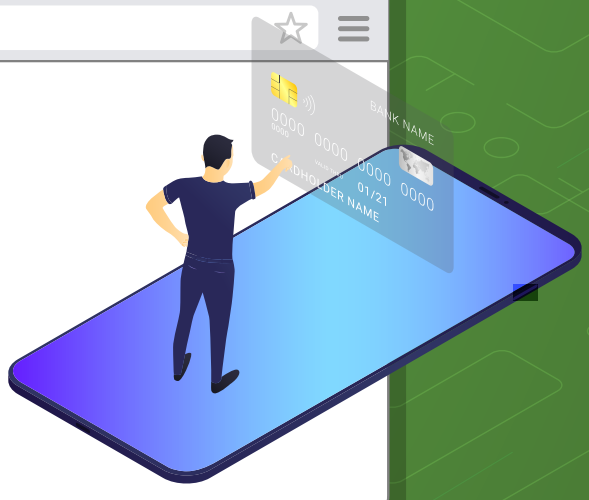
2). HINDARI BERTRANSAKSI MELALUI WARNET ATAU HOTSPOT AREA/ PUBLIC WIFI.

Hal ini dilakukan untuk menghindari sniffing terhadap segala aktivitas PermataBankers dengan PC/laptop, termasuk juga informasi rekening. Sniffing dapat diartikan penyadap paket dikenal sebagai Network Analyzers atau Ethernet Sniffer ialah sebuah aplikasi yang dapat melihat lalu lintas data pada jaringan komputer.

3). SATU KARTU UNTUK TRANSAKSI ONLINE.

Meskipun Nasabah mempunyai 5 Kartu Kredit, sebaiknya upayakan hanya satu kartu kredit yang sering digunakan belanja online. Hal ini selain kemungkinan Kartu redit lain "diintip," juga agar Nasabah dapat menghemat waktu memeriksa detail tagihan Kartu Kredit belanja online tersebut.

Saat ini, banyak Bank sudah menerapkan 3D secured, salah satunya PermataBank. Dengan sistem terbaru ini, Nasabah diharuskan menambahkan informasi "One-Time Password (OTP) yang akan diterima melalui SMS atau Pop-up Text di Ponsel Anda (dimana OTP ini akan berubah-ubah). Dengan adanya, tambahan pertanyaan informasi keamanan ini, Nasabah bisa lebih nyaman untuk bertransaksi secara online.



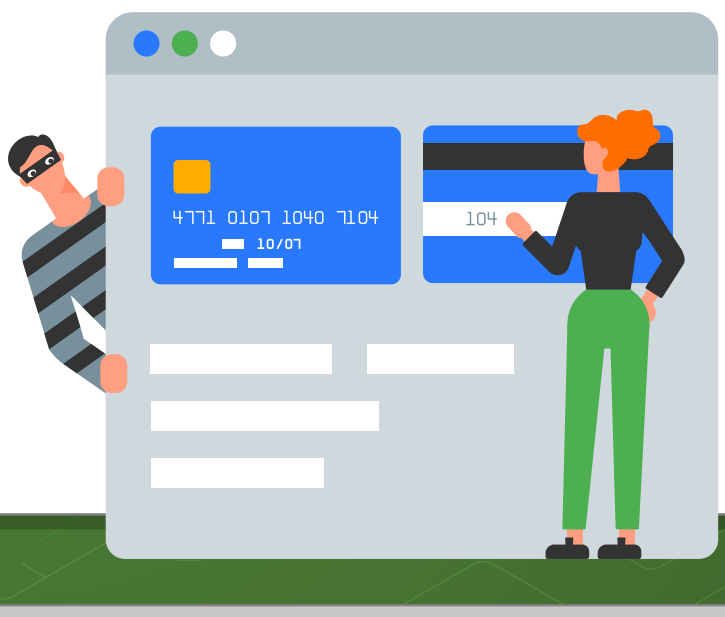
PENJELASAN SEPUTAR KEJAHATAN E-COMMERCE!

Carding pada e-commerce adalah suatu aktivitas belanja secara on-line (maya, dengan menggunakan data kartu debet atau kartu kredit yang diperoleh secara illegal. 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 informasi lainnya, si pelaku sudah dapat melakukan transaksi pada e-commerce.

CONTOH PENIPUAN

Pelaku mencari dan mendapatkan data-data kartu debit dan/atau kartu kredit. Untuk mendapatkan data-data tersebut, pelaku dapat melakukan dengan cara tertentu, misalnya marketing palsu, merchant palsu, pencatatan data-data sensitif oleh oknum pada merchant, ataupun dari kartu yang hilang.

Pelaku menggunakan data-data tersebut untuk berbelanja secara online. Transaksi terjadi dan tagihan akan dibebankan kepada Nasabah yang memiliki kartu dengan data-data yang telah digunakan secaa illegal oleh pelaku.



TIPS #3 - NASABAH JANGAN BERIKAN DATA RAHASIA KEPADA ORANG LAIN!

1. Simpan dan perlakukan Kartu Debit dan/atau Kartu Kredit dengan baik.
2. Anda harus menjaga rahasia/data/informasi transaksi, seperti PIN, TIN, Password, User ID, Response Code (Kode Otentifikasi Transaksi – One Time Password disingkat OTP), Card Verification Value (CVV) - berupa 3 digit angka terakhir di bagian belakang Kartu Kredit/Debit.
3. PermataBank tidak pernah meminta data/informasi rahasia tersebut, Nasabah wajib menjaga kerahasiaannya, dan tidak memberitahukannya kepada orang lain, termasuk karyawan/-petugas PermataBank.
4. 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.
5. Sebagai contoh, Anda wajib berhati-hati apabila tiba-tiba menerima SMS berisi kode OTP, walaupun Anda tidak melakukan transaksi dan kemudian dihubungi oleh seseorang yang mengaku dari PermataBank meminta kode OTP yang ada dalam SMS.
6. Apabila Anda menginformasikan kode OTP tersebut, sehingga transaksi dapat dilakukan oleh penelepon sebagai pelaku kejahatan, maka bank tidak akan bertanggungjawab terhadap transaksi yang terjadi.
7. Untuk menjaga keamanan data rekening saat Nasabah menghubungi petugas Contact Center, kini PermataBank telah memiliki teknologi Voice ID yang menggunakan pola suara untuk menghasilkan identifikasi unik dari setiap individu, yang dapat mempersingkat waktu proses verifikasi, sehingga kebutuhan Nasabah dapat segera ditangani. Untuk dapat menggunakan fasilitas verifikasi dengan Voice ID, Nasabah harus melakukan pendaftaran terlebih dahulu melalui PermataTel.
8. Apabila Anda menemui transaksi yang tidak wajar atau memerlukan informasi lebih lanjut, silahkan menghubungi PermataBank melalui :
   (i). PermataTel di nomor 1500-111, atau
   (ii). Mengunjungi cabang PermataBank terdekat, atau
   (iii). Email ke care@permatabank.co.id.