PermataBank

TIPS DATA AMAN NASABAH NYAMAN VOL.11

TIPS MENGHINDARI BAHAYA SOCIAL ENGINEERING TERUTAMA PHISHING!

Nasabah perbankan saat ini banyak dimudahkan dengan adanya *digital banking*, dimana Nasabah dapat melakukan transaksi perbankan, dimana saja, kapan saja, tanpa batas ruang dan waktu. Untuk itu, Bank telah menyiapkan infrastruktur yang didukung dengan sejumlah langkah untuk menjaga keamanan transaksi yang dilakukan Nasabah. Seperti pengiriman OTP ke nomor *handphone* Nasabah **yang telah terdaftar pada sistem bank**, sebelum terjadinya transaksi untuk mencegah terjadinya penyalahgunaan.

Umumnya, pelaku kejahatan berupaya menyiasati hal ini dengan melakukan *social engineering*, yaitu suatu teknik manipulasi secara psikologis yang digunakan oleh pelaku, **untuk mendapatkan informasi sensitif dengan tujuan negatif, seperti pencurian rekening bank, pencurian *password* atau *Personal Identification Number* (PIN), pencurian akun-akun tertentu, atau kejahatan lainnya.**

Contohnya, pelaku menelpon Nasabah dan menginformasikan bahwa Nasabah dapat menerima hadiah, jika menyebutkan kode OTP yang terkirim ke *handphone* (HP) Nasabah atas transaksi yang sebenarnya dilakukan oleh pelaku. OTP tersebut dapat berupa kode otorisasi transaksi *e-commerce* dan *internet banking*.

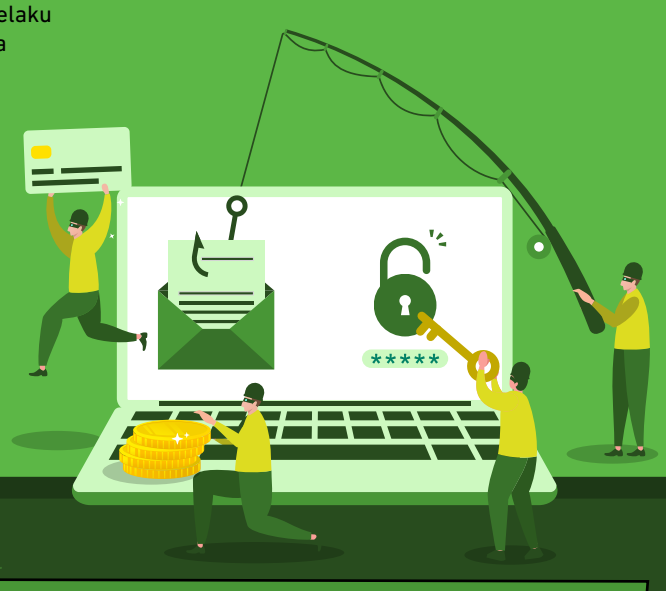
Oleh karena itu, Nasabah harus menjaga rahasia data/informasi transaksi, seperti *Personal Identification Number* (PIN), *Telephone Identification Number* (TIN), *Password*, *User ID*, *Response Code* (Kode Otentikasi Transaksi – *One Time Password* /OTP), *Card Verification Value* (CVV) – 3 digit angka terakhir di bagian belakang Kartu Kredit/Debit), juga nomor kartu atau tanggal kadaluarsa kartu (*expire date*).

Jika Anda menginformasikan informasi rahasia di atas, sehingga transaksi akhirnya dapat dilakukan oleh pelaku kejahatan, maka Bank tidak akan bertanggungjawab terhadap transaksi yang terjadi.

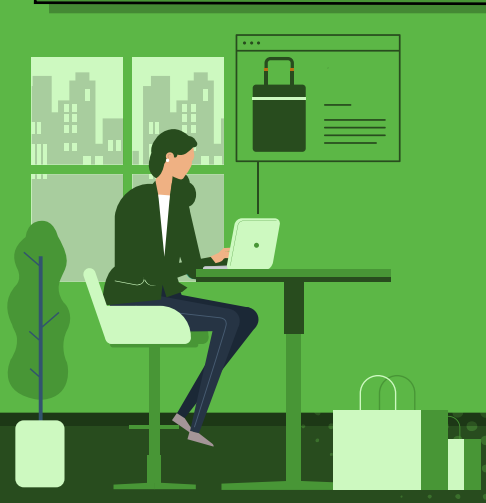
Demi keamanan bertransaksi Anda, maka jagalah kerahasiaan data transaksi tersebut.

ADAPUN JENIS SOCIAL ENGINEERING, MELIPUTI :

1. ***Shoulder surfing***, adalah suatu teknik mengamati target atau korban dengan tujuan mencuri data pribadi/PIN ATM/ password, dan lain-lain.
2. ***Phishing, Spear Phishing & Whaling Phishing***, adalah tindakan memperoleh informasi pribadi, seperti *user ID, password*, dan data sensitif lainnya dengan menyamar sebagai orang/organisasi yang sah melalui email dan mengarahkan korban meng-klik *link* palsu.
3. ***Spear Phishing***, adalah serangan melalui email yang seolah-olah dari rekan/organisasi yang telah kita kenal sebelumnya. Umumnya yang digunakan *hacker* untuk memperoleh nomor kartu kredit, nomor rekening, password dan informasi finansial lainnya.
4. ***Whaling***, adalah serangan *phishing* yang ditujukan untuk orang tertentu. Sepeti manajemen *executive* sebuah perusahaan, tokoh politik, artis-artis ternama, dan lain-lain.
5. ***Dumper diving***, adalah pencarian informasi/data penting dengan cara menggeladah tempat pembuangan sampah.
6. ***Skimming*** adalah aktivitas yang berkaitan dengan upaya pelaku untuk mencuri data dari pita magnetik kartu ATM/Debit secara ilegal, sehingga memiliki kendali atas rekening korban.
7. ***Vishing*** adalah suatu teknik yang menggunakan telepon untuk mengelabui/menipu Nasabah, agar mengungkapkan informasi pribadi dalam upaya mencuri identitas/melakukan penipuan. Umumnya, pelaku berpura-pura berasal dari sumber resmi, seperti bank atau organisasi Pemerintah.
8. ***Smishing***, adalah teknik yang menggunakan pesan teks ponsel (*short message services* – SMS) untuk memikat korban. Seringkali teks berisi URL atau nomor telepon. Nomor telepon seringkali memiliki sistem respon suara otomatis.
9. ***Tailgating*** adalah ketika orang yang tidak sah, secara fisik, mengikuti orang yang memiliki hak akses, agar dapat masuk ke area tertentu.



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



1). **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.

2). **Hindari bertransaksi melalui warnet atau hotspot area/public wifi.**
Lakukan transaksi hanya melalui jaringan yang terpercaya, seperti *home wifi* yang telah dienkripsi dengan *password*.

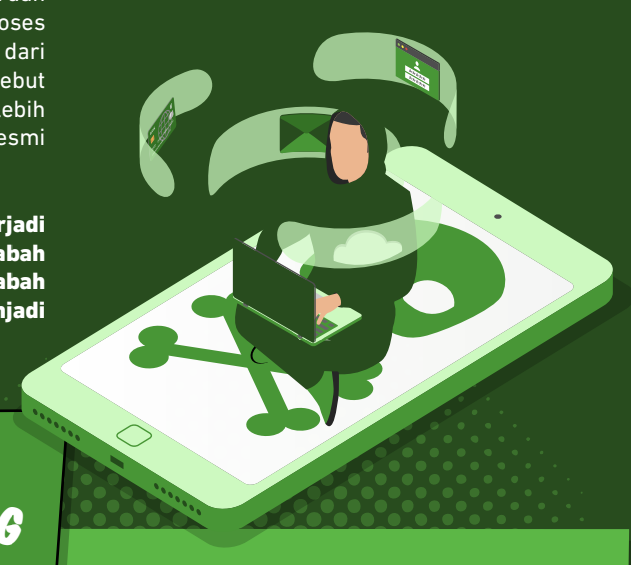
3). **Satu kartu untuk transaksi online.**
Walaupun nasabah memiliki lebih dari satu kartu, biasakan untuk menggunakan hanya satu kartu tertentu untuk transaksi *online*.

Salah satu modus *social engineering* yang sering dilakukan oleh pelaku kejahatan adalah dengan cara *Phising* yaitu tindakan meminta atau memancing pengguna komputer untuk mengungkapkan informasi rahasia, dengan mengirimkan pesan penting palsu, berupa : (i). *Email*, (ii). *website*, atau komunikasi elektronik lainnya.

Pesan palsu tersebut terlihat resmi dan meminta korban untuk segera mengirimkan/memberikan informasi yang diminta, supaya tidak terkena konsekuensi tertentu.

Selain itu, suatu *phishing* juga dapat ditandai dengan adanya kesalahan ketik dan gaya bahasa yang kurang baik. Umumnya, pesan *phising*, tidak melalui proses *review* dan *editing* yang baik. Bahkan, tidak jarang berupa terjemahan kasar dari bahasa asing. Namun demikian, sangat dimungkinkan pesan *phishing* tersebut menggunakan gaya bahasa yang baik untuk membuat Nasabah merasa lebih yakin dan percaya, bahwa pesan tersebut seolah-olah merupakan pesan resmi dari bank.

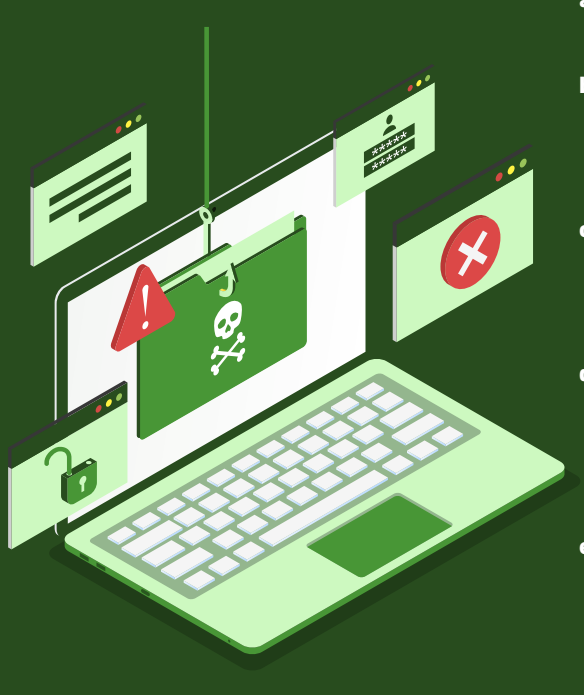
Contohnya, pelaku akan mengirimkan pesan : **"Saat ini, sedang terjadi pemeliharaan server untuk transaksi internet banking, sehingga Nasabah diminta untuk memasukkan berbagai data sensitif dan penting. Jika Nasabah tidak menginput data tersebut, maka rekening Nasabah tersebut akan menjadi tidak aktif dan tidak dapat digunakan."**



BERIKUT INI, TIPS MENGHINDARI BAHAYA PHISHING

(1). Jangan pernah mengirimkan informasi sensitif melalui email. Perlu diketahui, bahwa suatu perusahaan tidak akan meminta informasi sensitif melalui email atau sarana elektronis lainnya, yang tidak aman.
(2). **Jika terlanjur membalas email/SMS dari pelaku terindikasi phishing, segera lakukan penggantian password, PIN, dan data keamanan lainnya.**
(3). **Pastikan *Reference Code/Response Code* pada pesan *One Time Password* (OTP) yang diterima sama dengan *Reference Code/ Response Code* transaksi yang dituju. Hal ini terkait adanya modus *phishing* oleh *fraudster* dengan membelokkan *server* penginput kode OTP, salah satu cirinya adalah layar komputer/HP Anda berkedip.**
(4). Menggunakan *anti virus* yang terkini.
(5). Jangan mengklik link apa pun pada pesan (*email*) yang terindikasi *phishing*.
(6). Mengkonfirmasikan kepada pihak Bank, melalui Contact Center yang resmi, jika ada permintaan yang mencurigakan.
(7). Jangan pernah memasukkan user ID dan password pada suatu halaman *web* yang terbuka otomatis (**pop up**) atau dari *link*. Ketiklah alamat halaman *web* yang akan dibuka.
(8). Hati-hati mengunduh *attachment email*, karena dapat berisi *virus/malware*, yang dapat mencuri data sensitif.

SELAIN ITU, TERDAPAT JUGA BERAPA HAL YANG DAPAT DILAKUKAN UNTUK MENDETEKSI ADANYA PHISHING.



a. **Permintaan informasi pribadi melalui pesan email**
Waspadailah pesan yang meminta informasi pribadi atau informasi sensitif, sekalipun kelihatannya resmi.
b. **Menggunakan kata-kata yang mendesak**
Penggunaan kata dalam pesan *email* biasanya sopan dan bernada membantu. Pesan yang di sampaikan biasanya mendorong untuk membalasnya atau mengklik *link* dalam pesan. Seringkali pesan mendesak meminta, agar segera meresponnya tanpa berpikir.
c. **Terdapat Lampiran**
Kebanyakan skema pengelabuan (*phishing*) meminta untuk membuka lampiran, yang selanjutnya dapat menginfeksi komputer dengan *virus*. Lampiran yang ingin dlihat sebaiknya disimpan terlebih dahulu, lalu discan dengan *antivirus terupdate* sebelum membukanya.
d. **Link palsu atau mencurigakan**
Umumnya *phishing* akan menggunakan link tertentu yang dibuat sedemikian rupa untuk mengelabui Nasabah, dimana Nasabah akan meng-*click link* tersebut, tanpa menyadari bawah *link* tersebut palsu. Biasakan untuk mengunjungi website dengan alamat yang resmi, kemudian menyimpannya dalam menu *Favorite* di *browser*.
e. **Homograf**
Adalah kata yang sama ejaannya tetapi berbeda artinya. Pada komputer, yang dimaksud serangan *homograf* adalah alamat *web* yang terlihat seperti alamat *web* yang dikenal tapi sebenarnya telah diubah. Tujuan dari *link web* tipuan digunakan dalam skema pengelabuan (*phishing*), agar dapat mengelabui pengguna untuk mengklik *link* tersebut.

Untuk menghindari segala tindakan penipuan yang mengatasnamakan **Permata**Bank, maka Nasabah wajib merahasiakan data/informasi rahasia tersebut, serta tidak memberitahukannya kepada siapapun.

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 Andaa dapat diterima. Dan pastikan nomor HP yang Anda daftarkan untuk fasilitas OTP adalah nomor HP yang masih dipergunakan.

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.