Standard Chartered

Apakah Anda melihat apa yang kami lihat?

Selangkah lebih maju dari penipu.
Jangan biarkan mereka mengambil apa yang Anda miliki.

Kita berpikir bahwa hal tersebut tidak akan pernah terjadi pada kita—tapi pada kenyataannya penipu bertindak pada saat kita tidak memperhatikan. Mereka dapat mencuri informasi saat Anda berada di ATM atau saat Anda sedang online.

Penipu dapat meniru bank Anda, polisi, atau seseorang yang Anda kenal untuk membuat Anda membagikan data pribadi Anda atau mencuri uang Anda.

Mereka mungkin menghubungi Anda melalui surel, SMS atau telepon atau menggunakan malware untuk mengakses data Anda.

Di Standard Chartered, kami berkomitmen untuk membantu Anda untuk melawan penipuan sehingga penipu tidak bisa mengambil apa yang Anda miliki.

Rekayasa Sosial

Penggunaan *phishing*, *vishing* dan *smishing* untuk mengakses atau mendapatkan data pribadi Anda.

Phishing

Surel dengan tautan yang berisi *malware* yang dapat mengakses data pribadi Anda.

Vishing

Telepon berpura-pura dari pihak bank atau perusahaan untuk memperoleh detail akun.

Smishing

Pesan tertulis dari nomor yang tidak dikenal berisi tautan yang mencurigakan.

Tetap terlindungi dengan beberapa tips berikut:

- Perhatikan **alamat surel**. Perhatikan perubahan seperti johndoe@wahoo.com dibandingkan dengan johndoe@yahoo.com.
- Bertransaksilah pada **situs web yang aman** dengan ikon kunci atau tanda "*secure and verified*" yang terdapat pada halaman bawah situs web.
- Jangan pernah memberikan **data personal atau perbankan** kepada siapapun melalui telepon atau surel.
- Jangan meng-klik atau mengunduh *software* dari **tautan yang tidak dikenal**. Mereka bisa saja mengandung *malware* yang bisa mengakses informasi pribadi dari komputer atau telepon Anda.

SIM Porting/Swapping

Penipu dapat memperoleh duplikasi kartu SIM dari perusahaan telepon Anda dengan berpura-pura menjadi Anda. Ini memungkinkan mereka untuk menerima OTP dan pemberitahuan dari bank Anda.

Meminta duplikasi kartu SIM dengan alasan kehilangan telepon genggam, rusak atau penggantian kartu SIM.

Mengaktifkan kartu SIM baru untuk mengakses OTP/Notifikasi.

Tetap terlindungi dengan beberapa tips berikut :

- **Waspada terhadap segala notifikasi** yang dikirim oleh perusahaan telepon Anda atau adanya perubahaan kartu SIM yang tidak sah. Segera telepon mereka jika Anda menerimanya.
- Perhatikan jika Anda **kehilangan jaringan dalam jangka waktu yang lama**, bisa saja ini salah satu indikasi penonaktifan kartu SIM.

Penipuan ATM

Informasi kartu ATM Anda bisa saja dicuri saat Anda berada di ATM

Merusak dengan pembaca kartu untuk menangkap data kartu

Melihat dari belakang punggung Anda untuk melihat PIN Anda.

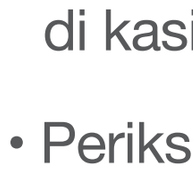
Memasang papan tombol palsu untuk mengambil PIN Anda.

Tetap terlindungi dengan beberapa tips berikut:

- **Tetap waspada** terhadap orang-orang di sekeliling Anda di ATM.
- Pastikan **mesin tidak dalam keadaan dirusak**.
- **Tutup papan tombol** saat Anda memasukkan PIN Anda.
- **Robek dan buang** tanda terima Anda.

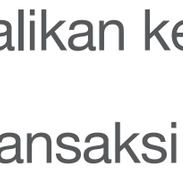
Penipuan Kartu

Penggunaan kartu untuk transaksi yang tidak sah dan melanggar hukum.



Menggunakan kartu hilang atau kartu dicuri untuk melakukan pembelian.

Menggunakan mesin *skimming* untuk menduplikasi detail kartu.



Transaksi *online* dengan menggunakan nomor kartu, tanggal kadaluarsa dan nomor CVV.

Berpura-pura sebagai pihak bank atau perusahaan telepon untuk memperoleh detail data kartu Anda.

Tetap terlindungi dengan beberapa tips berikut:

- Jangan pernah memberikan detail kartu Anda kepada siapapun.
- **Pastikan Anda tetap melihat kartu Anda** saat melakukan transaksi pembayaran di kasir dan pastikan kartu yang benar dikembalikan ke Anda.
- Periksa **laporan kartu Anda** untuk transaksi-transaksi yang tidak Anda ketahui.
- **Robek dan buang** laporan kartu, tanda terima, kartu lama dan kadaluarsa.

Penipuan terhadap orang lanjut usia

Target penipu bisa siapa saja termasuk orang lanjut usia.

Berpura-pura sebagai orang yang Anda sayangi dalam masalah dan meminta sejumlah uang.

Berpura-pura menjadi pekerja tukang yang ingin masuk ke rumah Anda dengan maksud untuk mencuri, atau bertindak sebagai konsultan keuangan untuk melakukan kecurangan terhadap simpanan Anda.

Menggunakan Rekayasa Sosial (Social Engineering) untuk mengakses data pribadi Anda.

Tetap terlindungi dengan beberapa tips berikut:

- **Abaikan** telepon atau surel yang menanyakan data pribadi atau data pembayaran.
- Selalu **verifikasi identitas** orang yang berhubungan dengan Anda.
- Jangan mengunduh **lampiran** apapun dari sumber yang tidak diketahui, mungkin lampiran tersebut mengandung *malware*.
- **Jangan membagikan** informasi pribadi, PIN atau password.

Pihak terlibat dalam pencucian uang

Seorang pihak yang terlibat dalam pencucian uang yang adalah pihak yang menerima dan mengirim uang dengan imbalan jasa. Penipu merekrut pihak untuk terlibat dalam pencucian uang dengan berbagai cara.

Melalui situs perjodohan. Diawali dengan pertemanan dan meminta mereka untuk mengirim uang atau membayar untuk hal-hal yang bernilai tinggi.

Melalui surel berpura-pura menjadi teman atau kenalan.

Melalui Sosial Media. Menawarkan kemudahan memperoleh uang untuk mendapatkan akses ke rekening Anda.

Tawaran pekerjaan yang meminta untuk menerima dan mengirim dana atas nama perusahaan.

Tetap terlindungi dengan beberapa tips berikut:

- Waspada terhadap orang yang menawarkan imbalan untuk menerima dan mengirim uang menggunakan rekening Anda.
- Jangan membuka rekening bank atas nama Anda untuk menerima atau mengirim uang untuk orang lain.

Penipu terkadang sulit untuk dikenali, namun bersama kita bisa mengurangi resiko dengan mengikuti beberapa tips berikut:

KENALI

TANDA MENCURIGAKAN

Jika ada keraguan, periksa pengirim informasi atau sumber dari telepon, surel dan/atau pesan.

HENTIKAN

AKTIVITAS MENCURIGAKAN

Jangan merespon permintaan informasi data pribadi sumber yang tidak dikenal/ terpercaya.

LAPORKAN

KEJADIAN

Jika Anda menduga adanya aktivitas penipuan, segera laporkan insiden tersebut. Semakin cepat penipu dilaporkan, semakin besar kesempatan untuk mencegah kerugian lebih lanjut.

#ApakahAndaMelihatApaYangKamiLihat