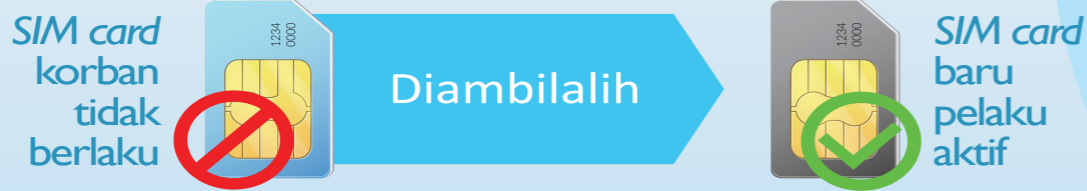




SIM SWAP Fraud adalah pengambilalihan *SIM card* korban oleh pelaku kejahatan, Sehingga yang kemudian aktif dan berlaku adalah *SIM card* baru pelaku, bukan lagi *SIM card* lama korban, biasanya digunakan oleh pelaku sebagai sarana untuk mengeksploitasi saldo bank korban.



Tips menghindari *SIM SWAP FRAUD*

STOP SHARE!
USER NAME, OTP, PIN, PASSWORD, KODE CVV/CVC KARTU KREDIT, pada siapa pun atau pihak yang mengatasnamakan institusi.

GANTI secara berkala semua jenis password Anda!

STOP mengumbar data pribadi Anda di media sosial.

JANGAN menginput data pribadi di situs palsu (*phising*).

JANGAN mudah tergiur dengan diskon atau hadiah besar, bisa jadi itu hanya umpan untuk memperoleh data pribadi Anda.

SITUS PALSU [PHISING]

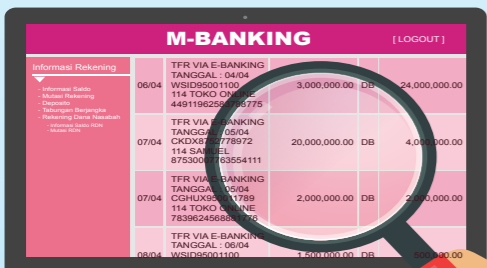
APLIKASI MALWARE

PESTA DISKON PALSU

OBRAL HADIAH PALSU

STOP SHARE

LANGKAH MENGHADAPI *SIM SWAP FRAUD*



GERAI BANK



Jika ada transaksi tidak dikenal yang mengurangi saldo bank anda, hubungi call center bank untuk meminta bank memblokir rekening anda. Lalu datang ke gerai bank untuk mendapatkan solusi lebih lanjut.

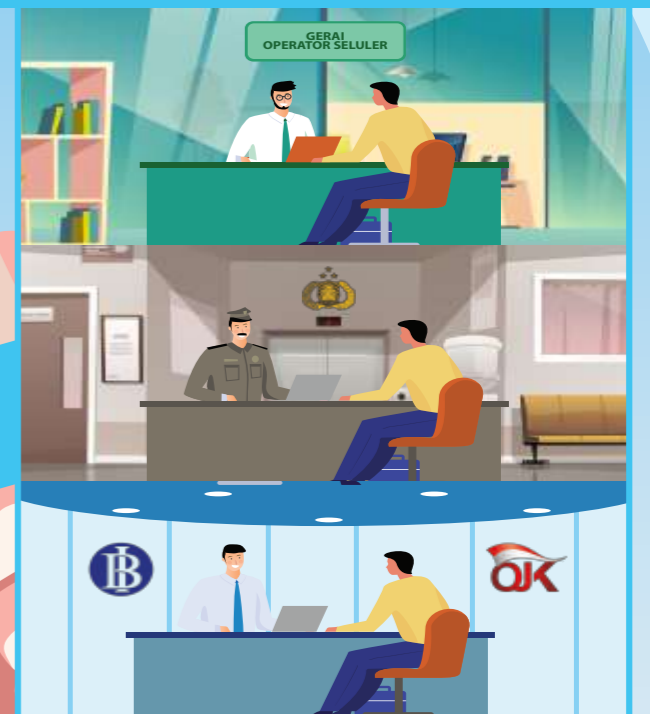


GERAI OPERATOR SELULER

Jika dibarengi dengan tidak berfungsinya simcard anda secara tiba-tiba, segera hubungi pihak operator seluler untuk menanyakan hal itu.



Jika ada pergantian *SIM card* yang tidak Anda ketahui, kemungkinan besar Anda terkena *SIM SWAP Fraud*. Mintalah operator seluler untuk memblokir *SIM card* di tangan pelaku.



Lalu ikuti prosedur penyelesaiannya dengan membawa *SIM card* lama Anda. Laporkan pada pihak berwenang untuk melengkapi pelaporan dan penyelidikan lebih lanjut.

Call Center Bank Indonesia : 131 | email : bicara@bi.go.id | Call Center OJK : 157 | email : konsumen@ojk.go.id

Info ini dipersembahkan oleh :



Bekerjasama dengan :



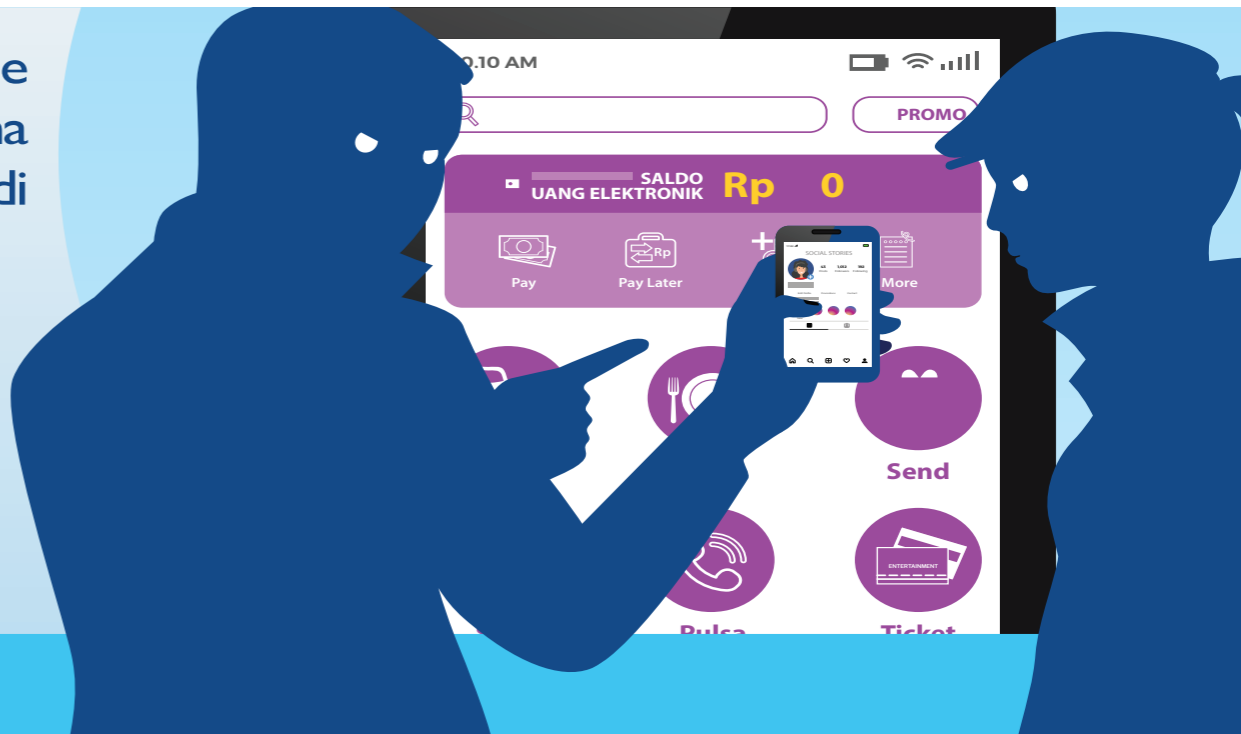


OTP (One Time Password) Fraud adalah pembajakan Kode Rahasia (OTP) korban oleh pelaku kejahatan, sebagai sarana untuk bisa mengeksploitasi uang elektronik atau uang di m-banking korban.

**ONE
TIME
PASSWORD
KORBAN**

DIBAJAK

**ONE
TIME
PASSWORD
PELAKU**



Langkah Menghadapi OTP FRAUD



Jika saldo uang elektronik /m-banking Anda tiba-tiba berkurang tanpa Anda ketahui, hubungi call center aplikasi uang elektronik atau uang m-banking terkait, untuk pengaduan dan penyelesaian.



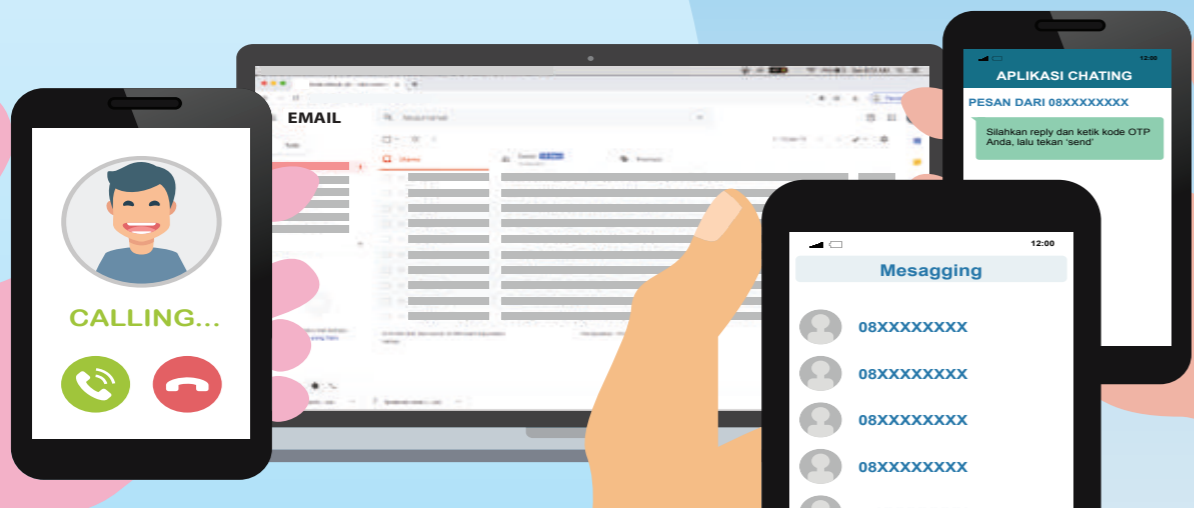
Jika ada transaksi tidak dikenal yang mengurangi saldo bank Anda, hubungi call center bank untuk meminta bank memblokir rekening Anda. Lalu datang ke gerai bank untuk mendapatkan solusi lebih lanjut.



Laporkan pada pihak berwenang untuk melengkapi pelaporan dan penyelidikan lebih lanjut.

TIPS MENCEGAH PENGAMBILALIHAN KODE RAHASIA (OTP FRAUD)

STOP SHARE! USER NAME, PASSWORD, PIN, KODE CVV/CVC KARTU KREDIT, terutama OTP (One Time Password) pada siapa pun atau pihak yang mengatasnamakan institusi.



WASPADA jika ada yang memintanya lewat email, aplikasi chat, telepon, maupun sms.

GANTI secara berkala semua jenis password Anda!

HATI-HATI membagikan data pribadi, apalagi diumbar di media sosial.

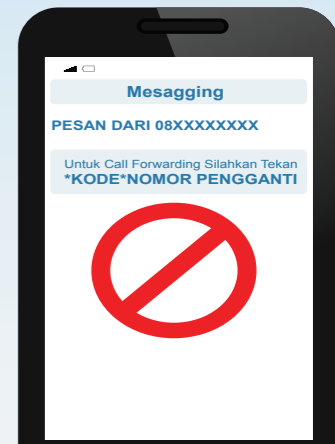
STOP menginput data pribadi Anda pada situs tidak jelas yang dicurigai sebagai hasil *phising*, yaitu situs palsu yang hanya ingin mengambil data pribadi Anda!

SITUS PALSU [PHISING] **APLIKASI MALWARE** **PESTA DISKON PALSU** **OBROL HADIAH PALSU**



JANGAN mudah tergiur dengan diskon atau hadiah besar, bisa jadi itu hanya umpan untuk memperoleh data pribadi Anda.

TOLAK jika ada yang menghubungi Anda dan meminta untuk menekan : *kode*Nomor Pengganti, bisa jadi itu adalah penipuan yang menggunakan fitur penerusan panggilan (*Call Forwarding*) untuk mengirimkan data telepon dan sms Anda pada pelaku!



Call Center Bank Indonesia : 131 | email : bicara@bi.go.id | Call Center OJK : 157 | email : konsumen@ojk.go.id

Info ini dipersembahkan oleh :



Bekerjasama dengan :

