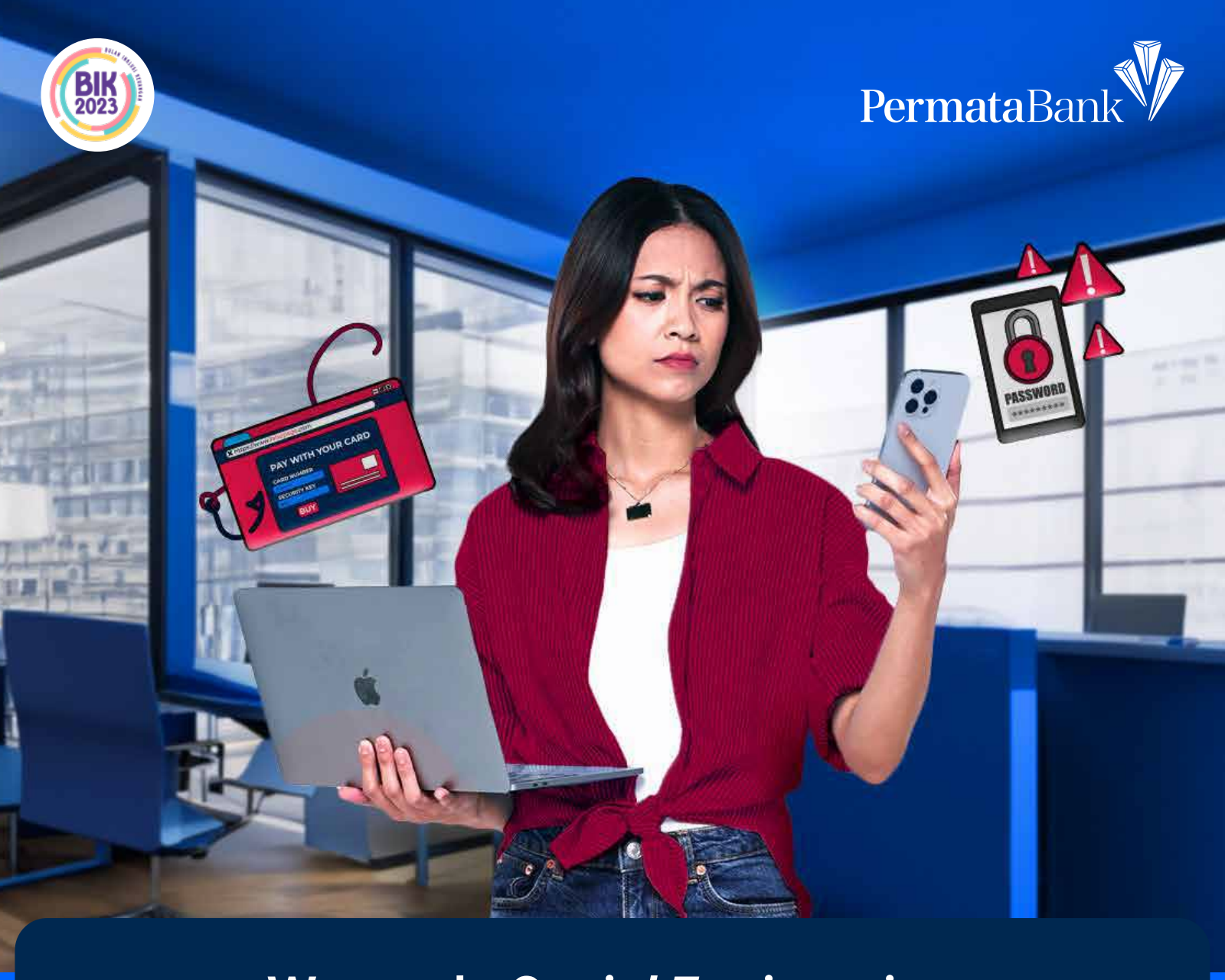
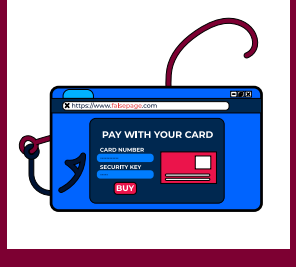


Waspada *Social Engineering* Jangan Sampai Kamu Jadi Korbannya!

Penipuan kini kian meresahkan, ada salah satu metode penipuan yang populer bernama *Social Engineering* atau rekayasa sosial, simak ulasan lengkapnya, biar kita bisa lebih waspada!

Social Engineering merupakan salah satu modus kejahatan dengan memanipulasi kondisi psikologis korban, korban biasanya dibuat sangat senang ataupun sangat panik terhadap suatu kondisi. Hal ini biasanya dimanfaatkan untuk menggali data informasi pribadi korban sampai dengan data perbankan.

Selalu berfikir rasional, lakukan verifikasi dan waspada terhadap hal yang memojokkan Anda melakukan sesuatu yang dilakukan secara mendadak. Kenali 2 penipuan *social engineering* berikut:



Phishing

Metode ini merupakan metode yang paling umum digunakan oleh para penipu untuk menjebak korbannya dengan cara menyamar sebagai pihak/organisasi yang resmi melalui *email* palsu, *chat* WhatsApp, telepon, atau media lainnya

Cara kerjanya yaitu dengan mengarahkan korban untuk mengklik *link* palsu, *download* & *install* sebuah aplikasi (.apk) yang sebenarnya adalah aplikasi *sms thief/sms spy/sms stealer* untuk memantau dan mencuri *Response Code/OTP (one time password)* serta *user ID* korban. Perlu kamu ketahui bahwa aplikasi tersebut selalu terkoneksi dengan *server* penipu, sehingga memudahkan penipu untuk menjalankan aksinya.

Skimming

Metode ini bertujuan untuk mencuri data kartu ATM Debit-Kredit dan PIN sehingga penipu memiliki akses ke rekening kamu.

Cara kerja *skimming* adalah dengan memasang beberapa alat tambahan seperti pembaca kartu ilegal (*skimmer*) di *card reader slot* (tempat memasukkan kartu pada pintu/mulut perangkat pembaca kartu), *keyboard* PIN ATM palsu yang melapisi *keyboard* asli mesin ATM/EDC milik Bank, dan kamera pengintai mini tersembunyi.

Karena itulah, penting untuk selalu waspada saat melakukan transaksi pembayaran belanja di *merchant* yang membutuhkan proses gesek/*swipe* kartu pada perangkat tambahan lain yang bukan mesin ATM/EDC. Pastikan bahwa mesin ATM/EDC yang digunakan untuk bertransaksi berada dalam kondisi normal dan tidak mencurigakan seperti tidak terdapat bekas cungkilan, lem, atau goresan.

Jika mendapatkan *chat*, SMS, telepon atau *email* mencurigakan yang mengatasnamakan **Permata**Bank, Anda bisa menghubungi:

PermataTel **1500-111** dan **021-29850611**

care@permatabank.co.id | @PermataCare

@PermataBank | PermataBank