

Social Engineering Bikin Merinding!

Di tahun 2022 ini masih ramai pemberitaan tentang kasus rekayasa sosial atau Social Engineering. Social Engineering adalah teknik manipulasi yang mengeksploitasi kesalahan manusia untuk mendapatkan informasi pribadi, akses, atau barang berharga.

Berikut jenis-jenis serangan *Social Engineering* yang sering digunakan:



Phishing

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.



Spear Phishing

Serangan melalui *email* yang seolah-olah dari rekan/ organisasi yang telah kita kenal sebelumnya, biasa yang digunakan *hacker* untuk memperoleh nomor kartu kredit, nomor rekening, *password*, dan informasi finansial lainnya.



Whaling

Serangan *phishing* yang ditujukan untuk orang tertentu seperti manajemen *executive* sebuah perusahaan, tokoh politik, artis-artis ternama, dll.



Shoulder Surfing

Teknik mengamati target atau korban dengan tujuan mencuri data pribadi/ PIN ATM/*password*, dll.



Vishing

Teknik yang menggunakan telepon untuk mengelabui/menipu nasabah agar mengungkapkan informasi pribadi dalam upaya mencuri identitas/ melakukan penipuan. Pelaku biasanya berpura-pura berasal dari sumber resmi, seperti bank atau organisasi pemerintah.



Smishing





Teknik yang menggunakan pesan singkat (SMS) untuk memikat korban. Sering kali teks berisi *URL* atau nomor telepon. Nomor telepon sering kali memiliki sistem respons suara otomatis.



Skimming

Aktivitas yang berkaitan dengan upaya pelaku untuk mencuri data dari pita magnetik kartu *ATM/debit* secara ilegal sehingga memiliki kendali atas rekening korban.

Jika ada aktivitas mencurigakan yang mengaku dari pihak **PermataBank**, segera hubungi:

-  PermataTel: 1500111
-  Email: care@permatabank.co.id
-  Twitter: @PermataCare
-  Facebook: PermataBank
-  Instagram: @permatabank