



Penipuan dengan Virtual Account

Setelah kita mengetahui modus penipuan yang menggunakan rekening Bank, ada juga penipu yang meminta dana untuk dikirim melalui *virtual account*. Tapi sebelumnya, kamu perlu tahu apa yang dimaksud dengan istilah *virtual account*. *Virtual account* adalah salah satu layanan *cash management* yang terdiri dari 16 nomor unik dan spesifik untuk membantu perusahaan yang menjadi nasabah PermataBank dalam mengidentifikasi penerimaan dana dengan proses rekonsiliasi secara cepat dan tepat. Penerbitan nomor *virtual account* tersebut dilakukan oleh perusahaan untuk selanjutnya diberikan kepada pelanggannya (perorangan maupun non perorangan) sebagai nomor rekening tujuan penerimaan dengan penamaan sesuai dengan nama pelanggan. Perusahaan pun dapat menjalin kerja sama dengan pelanggannya tanpa keterlibatan Bank.

Selanjutnya *virtual account* dapat digunakan pelanggan perusahaan (penyelenggara Keuangan) sebagai media penerimaan dana dari suatu transaksi tertentu. Ada 2 jenis *virtual account*, yaitu :



Static Virtual Account

Nomor *virtual account* yang bisa digunakan secara berulang, misalnya nomor *virtual account* untuk top up DANA, Shopeepay, Gopay, OVO dan lain sebagainya.



Dynamic Virtual Account

Nomor *virtual account* yang hanya bisa digunakan untuk satu kali transaksi, misalnya ketika melakukan pembayaran melalui *virtual account* di website online/e-commerce, misalnya transaksi melalui merchant facebook.

Karena *virtual account* dapat dijadikan media penerimaan dana, maka modus penipuan banyak terjadi menggunakan *virtual account*. Modus yang digunakan juga beragam, seperti yang pernah disampaikan pada materi edukasi sebelumnya, penipu bisa menggunakan modus seperti :

1



Mengaku sebagai kerabat atau teman

Tips : kenali gaya bicara/bahasa. Biasanya penipu terkesan sok kenal sok dekat dan mengutarakan sedang kena musibah atau dalam kondisi terdesak sehingga membutuhkan dana dalam waktu cepat.

2



Investasi melalui media sosial (whatsapp, telegram, dll)

Tips : Lakukan pengecekan penawaran investasi secara Legal dan Logis. Biasanya penawaran investasi yang menjanjikan keuntungan yang fantastis dan mengajak peserta mentransfer sejumlah dana melalui *virtual account*. Investasi yang ditawarkan tidak memiliki izin dan hasil investasi yang dijanjikan jauh dari harapan atau bahkan tidak ada. Adapun, skema tipuan berkedok investasi yang paling populer dan sederhana adalah skema Ponzi. Seorang promoter atau platform daring akan mengiming-imingi calon investor dengan tingkat imbal hasil (*return*) yang sangat tinggi.

3



Undian berhadiah palsu

Tips : Waspada dan gunakan Logika. Jika kamu tidak pernah mengikuti program hadiah tertentu, abaikan jika ada penelpon atau chat yang akan memberikan kamu hadiah, karena ujung-ujungnya penipu akan meminta data perbankanmu dan meminta sejumlah dana untuk mencairkan hadiah tersebut.

4



Belanja online atau toko online palsu

Tips : Lakukan *crosscheck* pada kolom komentar dan hindari pembayaran di luar metode pembayaran resmi dari toko online tersebut. Biasanya toko online palsu menonaktifkan kolom dan menampilkan testimoni palsu berupa *screenshot* chat Whatsapp, atau bahkan tidak ada testimoni sama sekali.

Cara cerdas menghindari modus penipuan di atas adalah :

1. Pada aplikasi *e-wallet* (yang menggunakan *virtual account*) terdapat fitur untuk dapat mengubah nama pemilik akun *e-wallet*, hal ini yang kemudian sering kali dimanfaatkan oleh *fraudster* untuk melakukan *social engineering* (penipuan). Sebelum melakukan transfer dana lebih baik hubungi dulu pemilik akun *e-wallet* untuk meminimalisir tindakan penipuan.
2. Jika ada pesan yang menyebut kamu memenangkan program undian berhadiah, pastikan kembali dengan menelepon *call center* Bank/ perusahaan. Cek apakah memang betul-betul menyelenggarakan program undian atau tidak.
3. Bertanya pada pakar/ahli keuangan dan investasi atau melakukan pengecekan produk keuangan kepada layanan pelanggan Otoritas Jasa Keuangan (OJK) sebelum memutuskan mengikuti penawaran investasi.
4. Perhatikan nama kontak dan gaya percakapan pengirim pesan. Jika ragu, sebaiknya blokir saja kontak nya
5. Hati-hati dengan *profile picture*, khawatirnya penipu menggunakan foto tersebut di akun *social media* lain untuk tujuan kejahatan.
6. Apabila terindikasi mengalami penipuan, segera hubungi *call center* Bank/perusahaan pemilik *virtual account* untuk pengecekan lebih lanjut dan sertakan bukti pelaporan berupa surat laporan dari kepolisian, bukti transaksi dan surat pernyataan.
7. Jika *virtual account* dirasa sebagai akun penampungan tindakan penipuan, segera laporkan akun tersebut melalui CekRekening.id milik Kementerian Komunikasi dan Informatika Republik Indonesia.

Informasi lebih lanjut, segera hubungi:

 care@permatabank.co.id |  PermataTel 1500-111 | 021 - 29850611

 @PermataCare |  @permatabank |  PermataBank