



WASPADA ⁸ INVESTASI ILEGAL

MENGAPA INVESTASI ILEGAL MASIH MARAK?



16.000+ pulau



Populasi
> 275 juta jiwa
(>50% generasi Z
dan milenial)



Pengguna internet
>210 juta



Indeks Inklusi Keuangan
75,02%

Indeks Literasi Keuangan
65,43%

Sumber: Survei Nasional Literasi
dan Inklusi Keuangan Tahun 2024

Survey SNLIK
2024

Gap
9,59 %



Literasi Digital Rendah
(Tahun 2021 peringkat
ke-56 dari 63 negara)

menurut data Institut for
Management Development dalam
World Digital Competitviness



Perilaku ingin praktis, tidak
teliti, malas membaca



Maraknya penawaran produk ilegal



Perilaku ingin cepat kaya
tanpa kerja keras

WASPADAI TAWARAN INVESTASI ILEGAL

CIRI-CIRI INVESTASI ILEGAL

1. Menjanjikan keuntungan tidak wajar dalam waktu cepat
2. Menjanjikan bonus dari perekrutan anggota baru “*member get member*”
3. Memanfaatkan tokoh masyarakat/ tokoh agama/ *Public Figure* untuk menarik minat berinvestasi
4. Klaim tanpa risiko (*free risk*)
5. Legalitas tidak jelas
 - a. Tidak memiliki izin usaha
 - b. Memiliki izin kelembagaan (PT, Koperasi, CV, Yayasan, dll) tapi tidak punya izin usaha.
 - c. Memiliki izin kelembagaan dan izin usaha namun melakukan kegiatan yang tidak sesuai dengan izinnnya.

PENYEBAB MARAKNYA INVESTASI ILEGAL

1. Pelaku
 - a. Kemudahan membuat aplikasi, web dan penawaran melalui media sosial
 - b. Banyak *server* di luar negeri
2. Masyarakat
 - a. Mudah tergir bunga tinggi.
 - b. Belum paham investasi

UPAYA SATGAS

UPAYA PENCEGAHAN

- Edukasi kepada masyarakat luas.
- *Crawling* data melalui sistem waspada investasi

UPAYA PENANGANAN

- Rapat koordinasi
- Mengumumkan investasi ilegal kepada masyarakat.
- *Cyber patrol* dan mengajukan blokir situs dan aplikasi secara rutin kepada Kominfo.
- Laporan informasi kepada Bareskrim Polri



Bagaimana dengan pengembalian dana masyarakat?

Cukup sulit, terutama apabila uangnya sudah digunakan oleh pelaku investasi ilegal atau sudah dibagi-bagi kepada *member-member* lama.



Apabila menerima penawaran investasi dengan iming-iming imbal hasil tinggi, kenali:



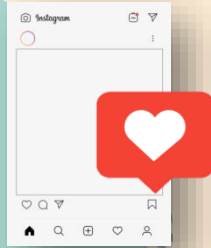
Legal: Status Perizinan (Badan Hukum & Produk)

Logis: Imbal hasil wajar dan memiliki risiko

MODUS INVESTASI ILEGAL

Money Game

Kegiatan like dan view post di media social dengan paket member dan referral



Contoh: Tiktok Cash, Batu Vulkanik, Golns, Like Share

Kegiatan E-commerce dengan sistem penjualan langsung

- Contoh:**
- PT Nunggal Tali Roso (NETERO)
 - PT Caturkerta Raharja (Belilapak.id)



Skema piramida dengan modus penjualan ebook

Contoh:

- Komunitas Jempol Preneur (KJP)/ Jempolpreneur.id
- Perpuskita/ Perpuskita.com
- Duit Bomber

Skema ponzi dengan modus belanja online

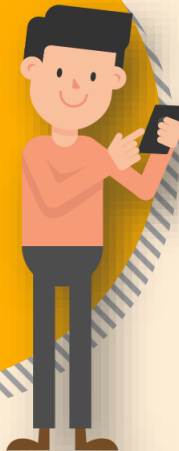


Contoh:

- JD Union
- Alimama Indonesia - almm.qdhtml.net/

Jasa pengisian isi ulang pulsa dengan memberikan bonus berjenjang

Contoh: PT Maestro Digital Telekomunikasi/ Maestro Pulsa, PT Duta Network Indonesia



Kegiatan jasa periklanan dengan sistem jaringan



Contoh:

- PT Kam And Kam (Memiles)
- PT Forkom Digital Indonesia (King Poin)

Skema ponzi dengan modus membantu sesama



Contoh:

- PT Asia Dynasty Sejahtera
- Dream 4 Freedom
- Autogajian

SOCIAL ENGINEERING

SCAM

Tindakan penipuan yang direncanakan pelaku untuk mendapatkan uang **melalui kontak komunikasi** seperti media chat dan telepon.



PHISING

Tindakan memancing pengguna komputer untuk mengungkapkan (*user ID, password/PIN, nomor serta masa berlaku kartu kredit, dan CVV*) dengan menggunakan **situs palsu**.



SMISHING

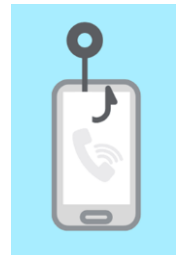
Tindakan penipuan **melalui pesan singkat atau SMS** yang bertujuan untuk mencuri informasi pribadi, keuangan, atau identitas korban.



12

VISHING

Tindakan penipuan **melalui telepon dengan berpura-pura menjadi customer service atau keluarga korban** untuk mengelabui korban.



SOCIAL ENGINEERING

Merupakan salah satu modus kejahatan dengan memanipulasi kondisi psikologis korban.
Rekening tabungan kita bisa dikuras tanpa kita sadari!

Info Perubahan Tarif Transfer Bank

Penipu berpura-pura sebagai pegawai bank dan menyampaikan informasi perubahan tarif transfer bank kepada korban. Penipu meminta korban mengisi *link* formulir yang meminta data pribadi seperti PIN, OTP, dan *password*.

Tawaran Menjadi Nasabah Prioritas

Penipu menawarkan iklan *upgrade* menjadi nasabah prioritas dengan segudang rayuan promosi. Penipu akan meminta korban memberikan data pribadi seperti Nomor Kartu ATM, PIN, OTP, Nomor CVV/CVC, dan *password*.

Akun Layanan Konsumen Palsu

Akun media sosial palsu yang mengatasnamakan bank. Akun biasanya muncul ketika ada nasabah yang menyampaikan keluhan terkait layanan perbankan. Pelaku akan menawarkan bantuan untuk menyelesaikan keluhannya dengan mengarahkan ke website palsu pelaku atau meminta nasabah memberikan data pribadinya.

Tawaran Menjadi Agen Laku Pandai

Penipu menawarkan jasa menjadi agen laku pandai bank tanpa persyaratan rumit. Penipu akan meminta korban mentransfer sejumlah uang untuk mendapatkan mesin EDC.

TIPS

Terhindar dari modus *sosial engineering*

1. Jangan mudah percaya apabila terdapat permintaan/pertanyaan *password*, PIN, OTP, MPIN, atau data pribadi.
2. Pastikan kembali ke *website*, *call centre*, dan *hotline* resmi.
3. Jangan sembarangan mengunduh aplikasi yang meminta akses terhadap seluruh data² di ponsel.
4. Blokir nomor telp dan/atau media sosial pelaku.
5. Laporkan ke pihak kepolisian apabila sudah mengalami kerugian

SOCIAL ENGINEERING - MODUS SNIFFING



OTORITAS
JASA
KEUANGAN

Apa itu

Modus *Sniffing*?

Modus penipuan *sniffing* adalah tindak kejahatan penyadapan oleh *hacker* yang dilakukan menggunakan jaringan internet dengan tujuan utama untuk mencuri data dan informasi penting seperti *username* dan *password m-banking*, informasi kartu kredit, *password email*, dan data penting lainnya.



OTORITAS
JASA
KEUANGAN

KENALI MODUSNYA!

Modus Penipuan *Sniffing* Berkedok Kurir Paket

- Pelaku berpura-pura menjadi kurir paket dan memberikan informasi palsu melalui pesan WhatsApp.
- Pelaku membuat tampilan aplikasi dalam bentuk *file* dengan memanipulasi memberikan nama "foto" untuk di buka, yang ternyata *file* tersebut adalah APK (aplikasi) berbahaya.
- *File* APK (aplikasi) yang dikirimkan pelaku jika diunduh akan melakukan *sniffing*/mengambil data dan informasi di ponsel korban secara ilegal yang digunakan untuk mengambil alih dan menguras rekening korban.



SEBELUM MEMILIH PRODUK/LAYANAN JASA KEUANGAN PASTIKAN



LEGAL



Pastikan produk/layanan memiliki **izin dari otoritas yang berwenang**



Pastikan penyelenggara memiliki **izin dalam menawarkan produk atau tercatat sebagai mitra pemasar**



Pastikan jika terdapat **pencantuman logo instansi/lembaga pemerintah sesuai dengan ketentuan yang berlaku**

15



LOGIS



Pastikan benefit dari produk-produk yang ditawarkan oleh perusahaan **masuk akal dan tidak ada indikasi penipuan**