



## Modul 3: Waspada Detektif Digital

Mengenal Penipuan dan Serangan Online – Pelajari cara mendeteksi, menghindari, dan melindungi diri dari ancaman digital yang semakin canggih.

MODUL 3

# Realita Pahit 2026: 10.583 Kasus dalam 90 Hari

10.583

Korban Tercatat

Data Bareskrim Polri, kuartal pertama 2026

90

Hari Saja

Lonjakan kasus dalam tiga bulan pertama tahun ini

1

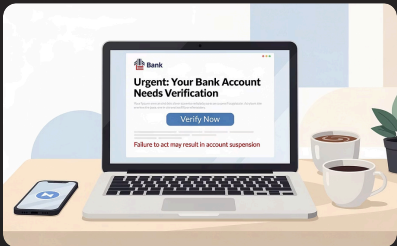
Target Utama

Perangkat pribadi Anda – bukan sistem korporat raksasa

Kejahatan digital telah beradaptasi dengan pola hidup masyarakat modern. Ancaman tidak lagi menyerang infrastruktur besar – kini langsung menarget smartphone dan akun pribadi Anda setiap hari.

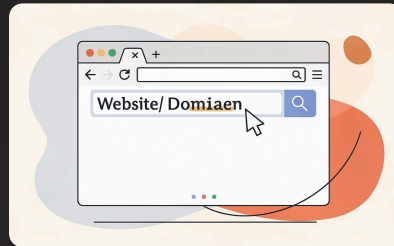


# Anatomi Penipuan: **Phishing & Smishing**



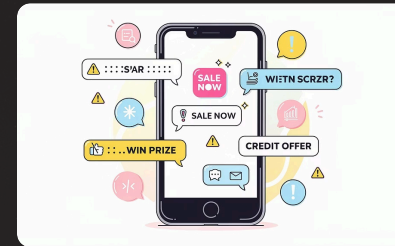
## Rekayasa Sosial

Memanipulasi korban agar percaya sedang berinteraksi dengan pihak resmi seperti bank, pemerintah, atau e-commerce.



## Tautan Palsu

Teknik **typosquatting** – domain seperti `bank-bca-pusat.xyz` dibuat semirip mungkin dengan situs resmi.



## Media Serangan

SMS, WhatsApp, dan email dengan iming-iming hadiah atau ancaman pemblokiran rekening untuk memancing kepanikan.

ANCAMAN NYATA

# Jebakan di Balik WhatsApp



## Modus APK Berbahaya

File .apk disamarkan sebagai undangan pernikahan, surat tilang ETLE, atau foto paket kiriman.

## Dampak Instan

Aplikasi jahat mencuri kode OTP dan menguras saldo m-banking dalam hitungan menit tanpa disadari.

## Prinsip Pertahanan

Jangan pernah mengklik atau menginstal file dari nomor tak dikenal, sekecil apa pun risikonya tampak.

# Penipuan Korporat & Profesional



## Business Email Compromise

Penipu menyamar sebagai pimpinan atau klien terpercaya untuk mengalihkan pembayaran dana ke rekening palsu.




## Fake Invoice

Tagihan palsu dikirim dengan urgensi tinggi agar dibayar segera tanpa sempat melalui proses verifikasi internal.



## Deepfake & AI

Suara atau wajah sintetis digunakan untuk menciptakan kepanikan keluarga atau instruksi palsu yang meyakinkan.

 Serangan ini menasar profesional dan karyawan keuangan – siapa pun bisa menjadi korban tanpa kewaspadaan yang tepat.



# Mengapa Kita **Sering Terjebak?**

Penipu tidak meretas teknologi – mereka meretas **psikologi manusia**. Memahami taktik mereka adalah pertahanan terkuat Anda.

1

## Urgensi Palsu

"Rekening Anda diblokir dalam 24 jam!" – memaksa tindakan impulsif tanpa pikir panjang.

2

## Tekanan Psikologis

Korban dipaksa bertindak cepat sebelum sempat berpikir jernih atau berkonsultasi dengan orang lain.

3

## Eksplorasi Rasa Penasaran

Iming-iming hadiah besar atau dokumen penting tak terduga yang memancing korban untuk mengklik tautan.

# Studi Kasus: Bedah Pesan Penipuan



Tiga langkah ini dapat diterapkan dalam detik pertama saat menerima pesan mencurigakan – sebelum Anda bereaksi secara impulsif.

## Tanda-tanda Pesan Penipuan

- Alamat pengirim menggunakan domain gratis atau typo (misalnya `support@bca-helpdesk.xyz`)
- Tautan tidak sesuai dengan domain resmi institusi yang diklaim
- Lampiran berekstensi `.apk`, `.exe`, atau `.zip` yang menyamar sebagai gambar/dokumen
- Bahasa yang penuh tekanan, kesalahan tata bahasa, atau tanda baca tidak wajar

⊗ Jika ragu, **jangan klik**. Selalu verifikasi melalui saluran resmi sebelum mengambil tindakan apa pun.



## PERLINDUNGAN DIRI

# Cara Memverifikasi Informasi

Kebiasaan sederhana ini dapat mencegah kerugian besar. Verifikasi selalu menjadi langkah pertama sebelum bertindak.

- Cek legalitas investasi di [ojk.go.id](http://ojk.go.id) atau [bi.go.id](http://bi.go.id) sebelum percaya tawaran apapun
- Tidak ada pihak resmi yang meminta OTP, PIN, atau password melalui pesan atau telepon
- Aktifkan **otentikasi dua faktor (2FA)** sebagai lapisan keamanan ekstra di semua akun penting

# Langkah Mitigasi Jika **Menjadi Korban**



## Putus Komunikasi Segera

Hentikan semua interaksi dengan pelaku. Jangan kirim uang tambahan meskipun dijanjikan pengembalian dana.



## Simpan Semua Bukti

Ambil tangkapan layar percakapan, riwayat transaksi, dan nomor rekening pelaku untuk keperluan penyelidikan.



## Laporkan & Blokir Akses

Laporkan ke Bareskrim ([patrolisiber.id](https://patrolisiber.id)) dan segera hubungi bank untuk membekukan transaksi yang terdampak.



# Jadilah **Benteng Terakhir** Keamanan Digital



## **Tidak Ada Kekayaan Instan**

Setiap penawaran yang terlalu muluk adalah indikasi kuat penipuan. Waspadaai iming-iming keuntungan tidak masuk akal.

## **Kewaspadaan Adalah Kunci**

Keamanan siber bukan sekadar teknologi – ini tentang kebiasaan dan kewaspadaan manusia setiap hari.

## **Jadilah Agen Perubahan**

Bagikan pengetahuan ini kepada keluarga, rekan kerja, dan komunitas Anda untuk menciptakan perlindungan kolektif.

Satu orang yang waspada dapat melindungi seluruh komunitas dari ancaman digital.