Mengenal Risiko di Balik

Like dan Share

Keamanan dalam Berinteraksi di Media Sosial

WHO AM I

- IT Security Specialist
  PT. Integrity Indonesia
- Practitioner Lecturer
  Institut Teknologi Budi Utomo Jakarta (ITBU)

- Budi Wibowo -

Cyber Security Enthusiast | Security Analyst Researcher | Lecturer

- NSE 1 Network Security Associate
- NSE 2 Network Security Associate
- Certified Ethical Hacker (CEH)
- Certified Network Security Specialist (ICSI)
- ISO/IEC 27001 Information Security Associate
- AWS Cloud Practitioner Essentials
- Cisco Certified CyberOps Associate

Scopus – ID: 57194020685
URL: https://www.scopus.com/authid/detail.uri?authorId=57194020685

Google Scholar: Budi Wibowo – H-Index: 2
URL: https://scholar.google.com/citations?hl=id&user=g0JSdZYAAAAJ

Sinta RistekBRIN – ID: 6756792
URL: https://sinta.kemdikbud.go.id/authors/profile/6756792

IG :@budi_wibowo93
Linkedin:@budiwibowo-
Email : budiwibowo1993@gmail.com

Cybersecurity researchers who still want to learn and share.

Introduction

Media sosial telah menjadi bagian penting dalam kehidupan sehari-hari. Kemampuan untuk berbagi informasi, foto, dan opini dengan cepat dan mudah telah mempermudah komunikasi.

Namun, di balik kemudahan ini, terdapat risiko yang tersembunyi. Ancaman seperti phishing, malware, dan rekayasa sosial dapat mengancam keamanan pengguna.

Pernahkah Anda berpikir bahwa satu klik like atau share bisa berdampak besar?

Ancaman Tersembunyi di Balik Like dan Share

Phishing

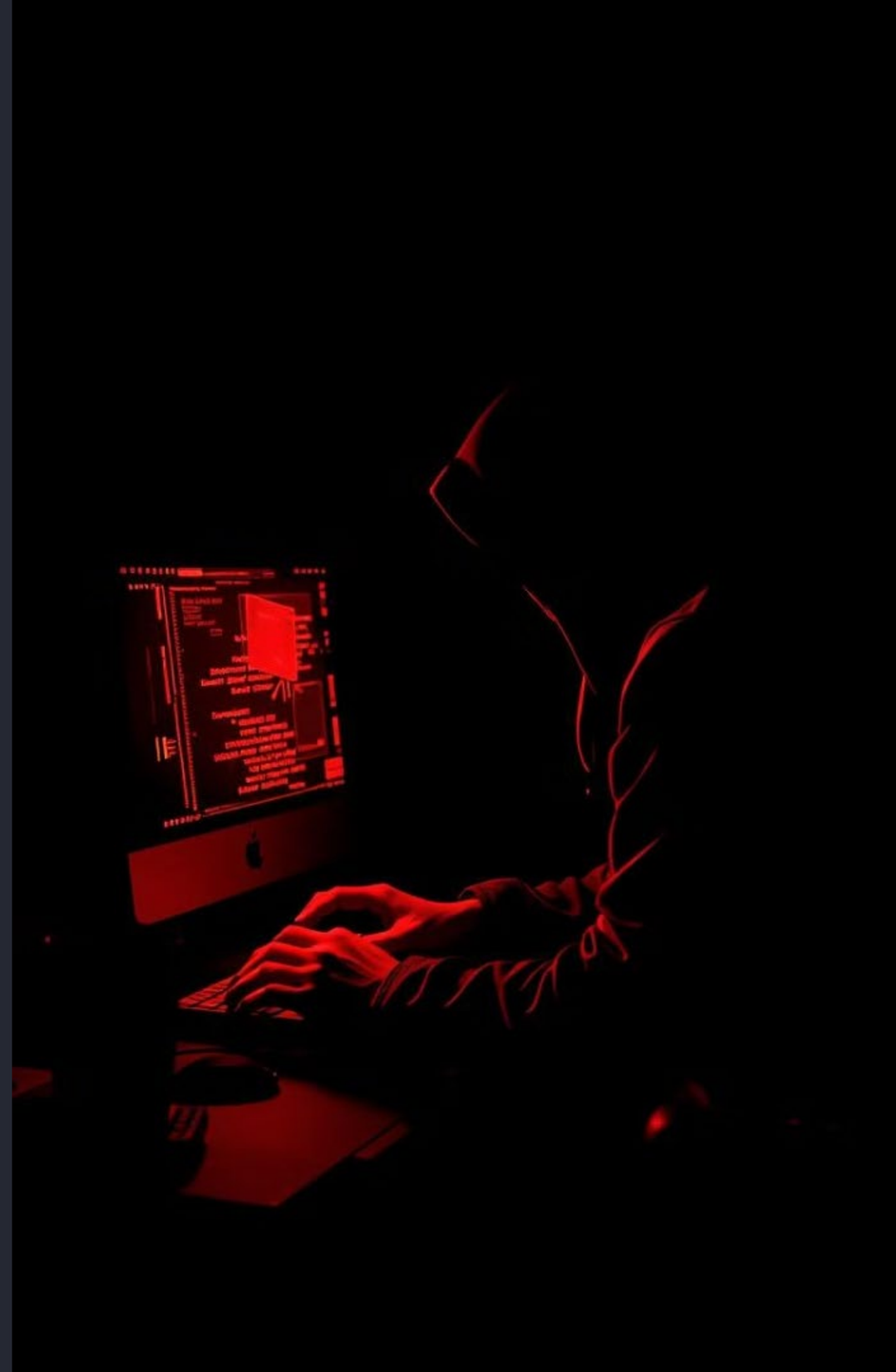
Penipuan yang mencoba mencuri data pribadi melalui pesan atau link palsu.

Malware

Perangkat lunak berbahaya yang bisa mencuri informasi atau merusak perangkat.

Rekayasa Sosial

Manipulasi psikologis untuk mendapatkan data pribadi atau akses ke akun.



Risiko Nyata dari Aktivitas Like dan Share

Meningkatkan Eksposur

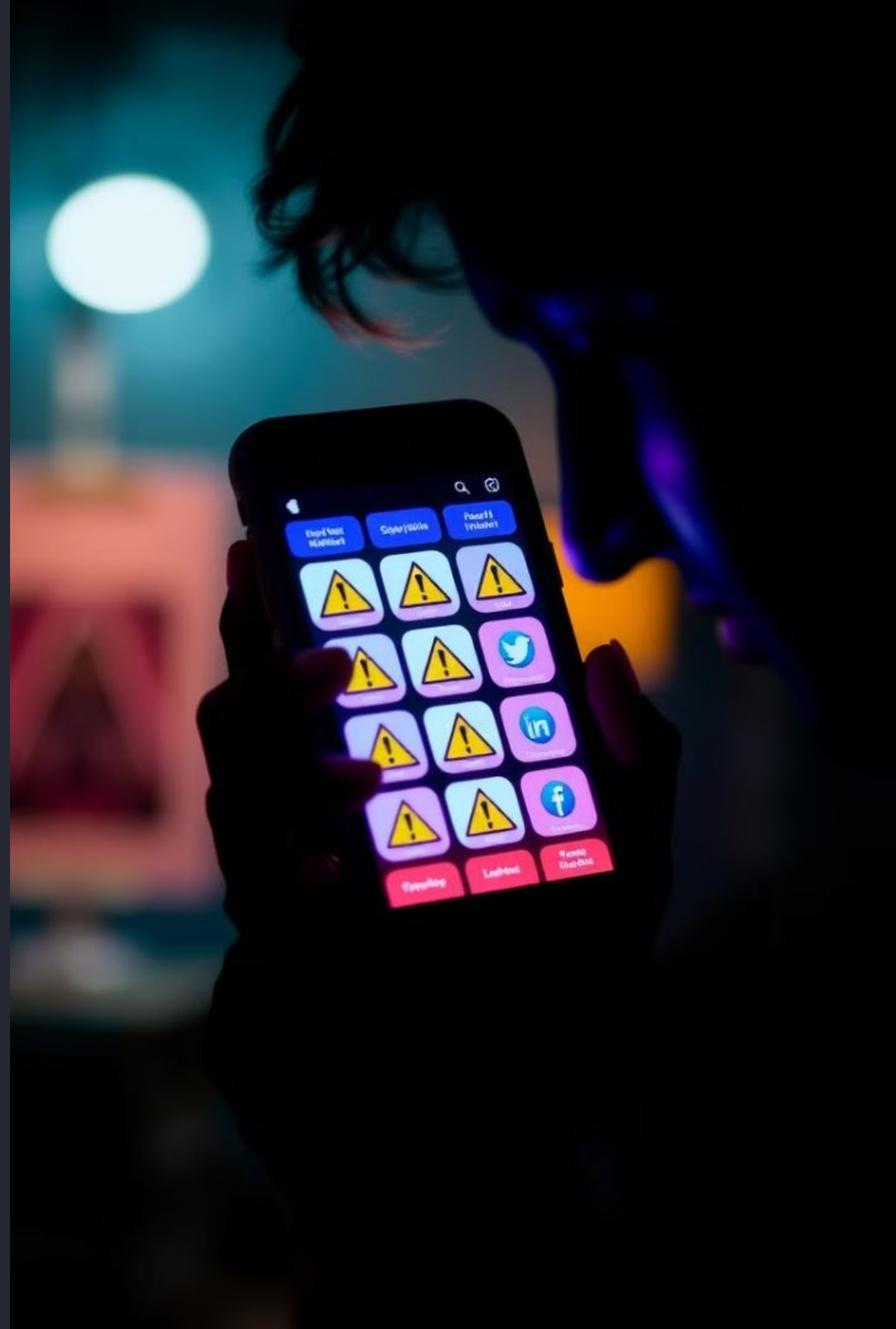
Aktivitas seperti dan bagikan dapat memberikan akses kepada pihak tidak bertanggung jawab untuk melacak kebiasaan pengguna.

Menyebarkan Informasi Palsu

Tanpa sadar, pengguna dapat menyebarkan hoaks yang merugikan orang lain atau merusak reputasi.

Menjadi Korban Penipuan

Penawaran palsu yang muncul di timeline akibat algoritma media sosial dapat membuat pengguna tertipu dan kehilangan uang.



Contoh Kasus - Penipuan Pekerjaan Online

Waspadai Tawaran

Pekerjaan dengan gaji tinggi tanpa keahlian biasanya mencurigakan.

Jangan Pernah Membayar

Perusahaan resmi tidak akan meminta bayaran untuk proses rekrutmen.

Verifikasi Identitas

Periksa situs web resmi dan testimoni dari karyawan sebelum menerima tawaran.

Hindari Membagikan Data

Data seperti KTP, rekening bank, atau nomor telepon bisa disalahgunakan untuk penipuan.

Ciri-Ciri Penipuan Like , share & Subscribe

Janji Keuntungan Besar

Pekerjaan ringan dengan keuntungan besar

Kedok E-commerce

Menggunakan nama e-commerce besar

Meminta Transfer Uang

Korban diminta mengirim uang

Pelaku Menghilang

Pelaku menghilang setelah korban menyetor uang

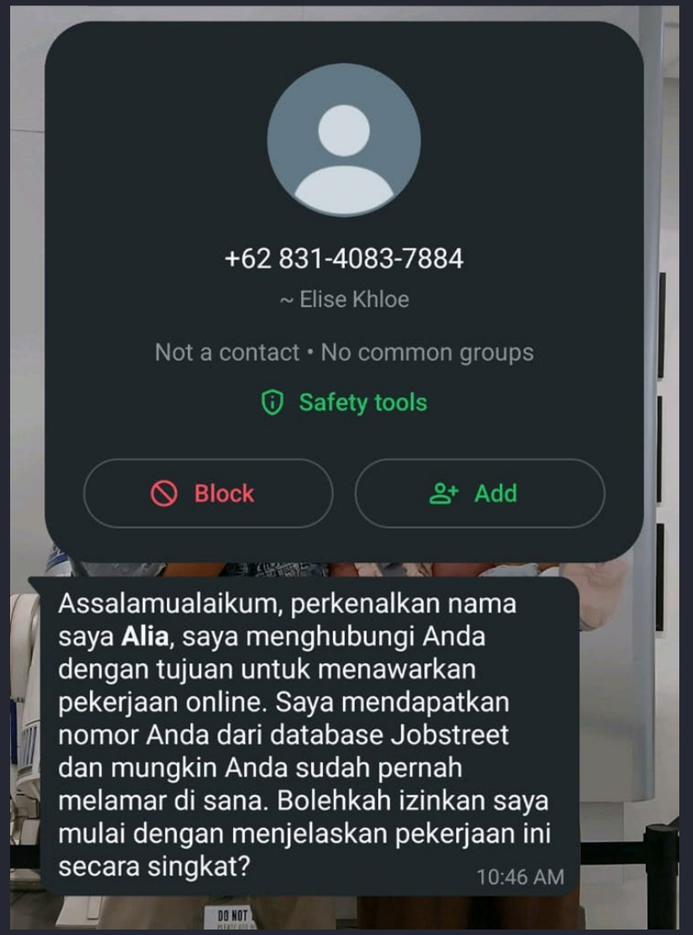
Penipuan Berkedok Like & Subscribe

Modus Baru

Penipuan mengincar masyarakat di Jabodetabek

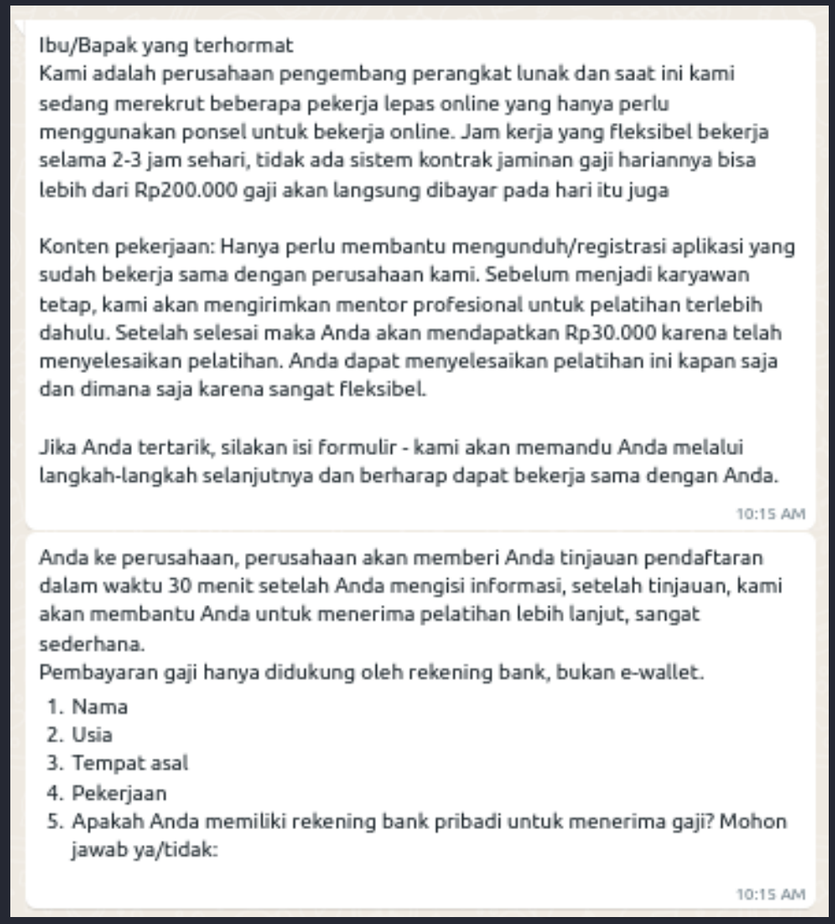
Janji Manis

Korban dijanjikan komisi besar



Modus Operandi

Korban diminta menyetor uang



Bagaimana Modus Ini Bekerja?

1. Korban melihat iklan pekerjaan online
2. Tugas awal: like, subscribe, atau review
3. Pelaku mengirim komisi kecil
4. Tugas meningkat, korban diminta membeli barang atau mentransfer uang
5. Pelaku menghilang

Dampak bagi Korban

Kerugian Finansial

Uang tidak bisa dikembalikan

Dampak Psikologis

Korban mengalami stres

Data Pribadi Berisiko

Informasi korban disalahgunakan

Penyalahgunaan Akun

Akun korban dipakai untuk kejahatan lain

Apa yang Harus Dilakukan Jika Terjebak?

1

Hentikan Komunikasi

Segera hentikan komunikasi dengan pelaku

2

Hentikan Transaksi

Jangan melakukan transaksi lebih lanjut

3

Ubah Password

Segera ubah password jika merasa akun Anda diretas.

4

Sebarkan Informasi

Sebarkan informasi kepada keluarga dan teman

Apa yang Harus Dilakukan Jika Terjebak?

5

Scan Perangkat

Scan perangkat dengan antivirus jika menduga terkena malware.

6

Laporkan

Laporkan akun atau pesan mencurigakan ke platform media sosial.

7

Jangan Panik dan Tetap Tenang

Dokumentasikan bukti - bukti berupa chat atau transfer ke rekening pelaku

8

Hubungi Pihak Berwenang

Hubungi pihak berwenang jika mengalami penipuan online.

Cara Mencegah dan Mengurangi Risiko

Mengenali Tautan Berbahaya

Jangan klik tautan dari sumber yang tidak dikenal. Periksa URL sebelum membuka tautan.

Mengamankan Akun Media Sosial

Aktifkan autentikasi dua faktor (2FA). Gunakan password yang kuat dan unik. Jangan membagikan informasi sensitif di media sosial.

Verifikasi Informasi Sebelum Membagikan

Cek fakta menggunakan sumber terpercaya. Hindari membagikan informasi yang tidak diverifikasi.

Hindari Oversharing

Jangan membagikan terlalu banyak informasi pribadi. Batasi audiens untuk setiap postingan.

Bagaimana Melindungi Diri?

1 **Waspada**

Jangan asal klik tautan yang tidak dikenal.

2 **Password Kuat**

Gunakan password yang kuat dan berbeda untuk setiap akun.

3 **Aktifkan 2FA**

Aktifkan Autentikasi Dua Faktor (2FA) untuk keamanan tambahan.

4 **Periksa Keamanan**

Periksa keamanan situs web sebelum memasukkan informasi pribadi.

5 **Jangan Mudah Membagikan**

Jangan mudah membagikan informasi pribadi di media sosial.

Edukasi dan Literasi Digital

1. Tingkatkan kesadaran akan risiko media sosial. Ikuti kursus atau seminar tentang keamanan digital untuk memahami ancaman dan cara mengatasinya.

2. Ajarkan keluarga dan teman cara berinteraksi yang aman di media sosial. Bagikan tips dan trik untuk menghindari risiko.

Penutup

1

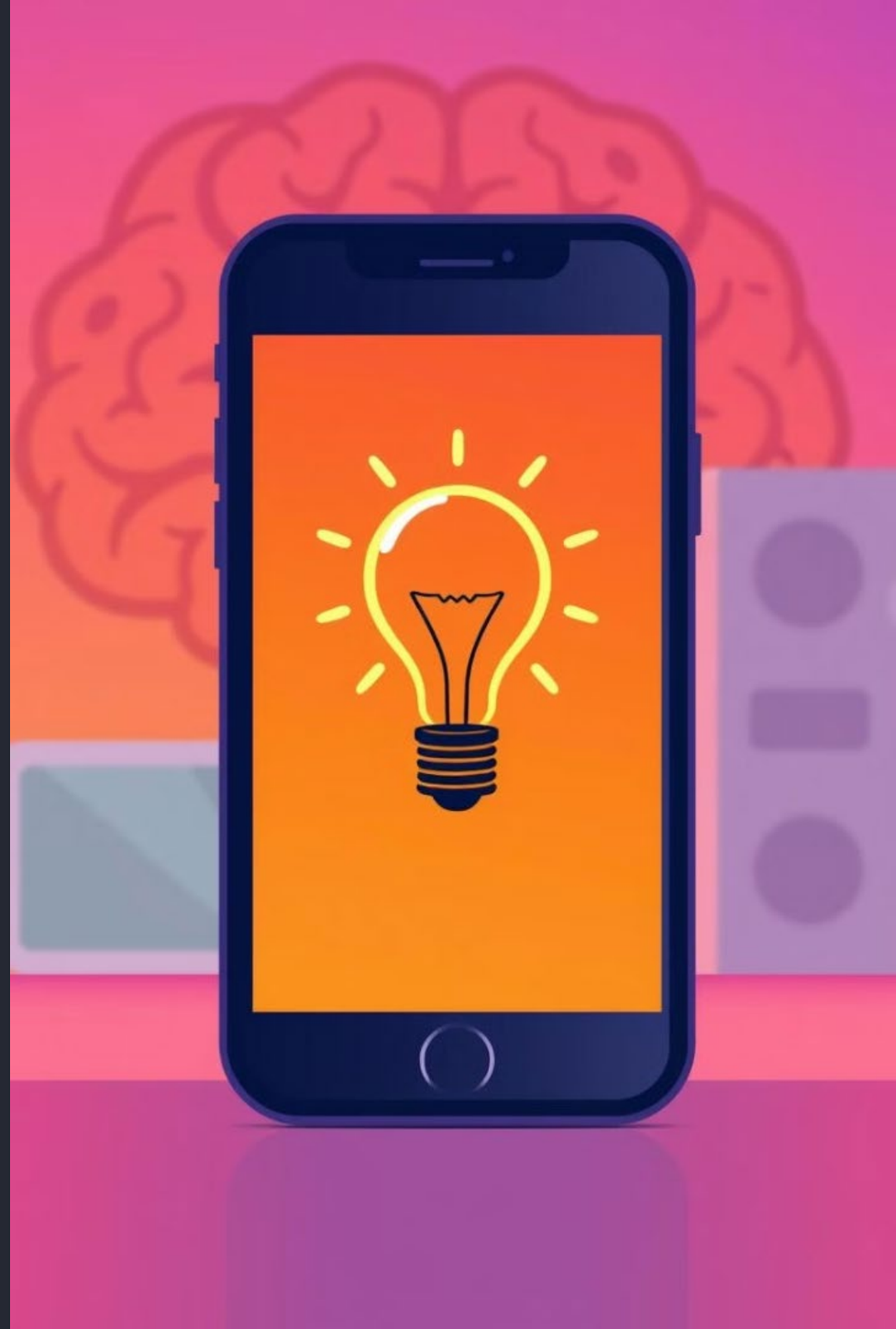
Media Sosial yang Bijak

Media sosial adalah alat yang bermanfaat jika digunakan dengan bijak. Ketahui risiko yang ada dan lindungi diri dari ancaman.

2

Langkah Pencegahan

Terapkan langkah pencegahan untuk melindungi diri dari phishing, malware, dan rekayasa sosial. Selalu waspada dan berhati-hati.



Q&A: Ada Pertanyaan?

Sesi tanya jawab ini adalah kesempatan untuk membahas kekhawatiran peserta dan mendapatkan jawaban yang spesifik.

Terima Kasih