

# Waspada Ancaman Siber pada Penggunaan Aplikasi Perbankan dan Dompot Digital

**Juan Intan Kanggrawan**

Technology & Public Sector Transformation Expert

Past Experience:

Head of Data-Product-Research-Operation (Smart Cities & National Ministry)

# Intro

<https://www.juan-kanggrawan.com>



**Juan Intan Kanggrawan**  
Head of Digital Products & Data Analytics

  
jakarta smart city

+62813 9887 6737  
+65 9123 9445 (WhatsApp)

Juan.tan.kang@gmail.com  
Juan.intan@jakarta.go.id

Jakarta Smart City  
Jakarta Provincial Government Administration  
<https://smartcity.jakarta.go.id/en>



**Juan Intan Kanggrawan**  
Head of Digital Products & Tribe/Operation  
*(Data Ecosystem, Rapor Pendidikan, Higher Education, Research, Central Platform, Belajar.id)*


+62813 9887 6737  
+65 9123 9445 (WhatsApp)

Juan.tan.kang@gmail.com  
Juan.kanggrawan@wartek.belajar.id

GovTech: Kementerian Pendidikan, Kebudayaan, Riset & Teknologi  
*(GovTech: Ministry of Education, Culture, Research & Technology)*  
<https://www.kemdikbud.go.id>

# Intro



**Ministry of Education, Culture, Research, Technology**  
Head of Digital Products & Tribe/Operation



**Jakarta Smart City (Jakarta)**  
Head of Digital Products & Data Analytics



**Traveloka (Singapore)**  
Analytics Lead, Senior Data Product Manager



**Sense Infosys (Singapore)**  
Assistant Director (Analytics Products)



**Icon Business Solutions (Singapore)**  
Pre-sale Lead, Assistant VP (Analytics)



# *Latest Technology Trend*

# Latest Technology Trend

## Technology trends and underlying technologies

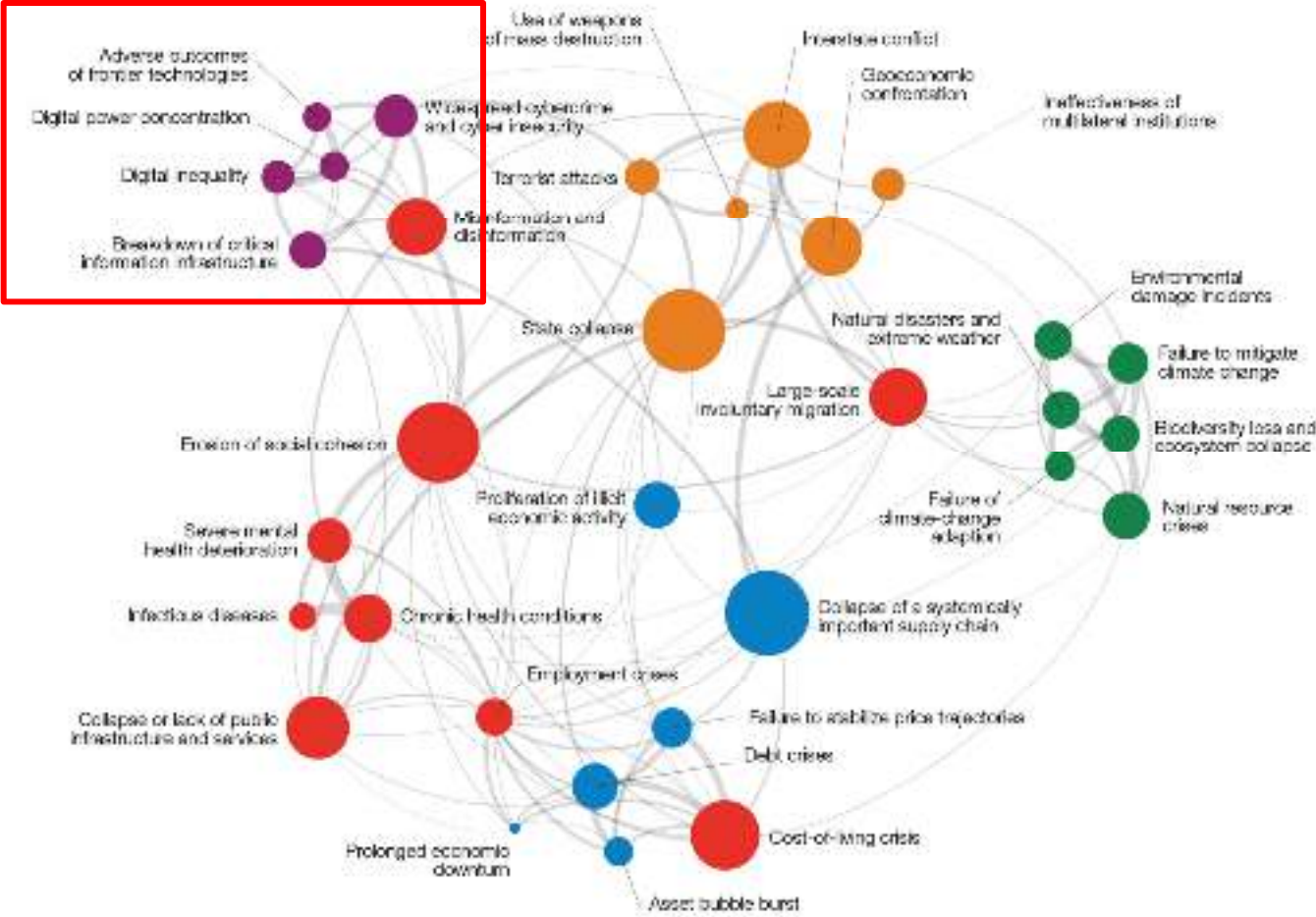
Industry-agnostic trends

 <b>1</b> <b>Next-level process automation...</b> Industrial IoT <sup>1</sup> Robots/cobots <sup>2</sup> /RPA <sup>3</sup>	 ... and process virtualization Digital twins 3-D/4-D printing	 <b>2</b> <b>Future of connectivity</b> 5G and IoT connectivity	 <b>3</b> <b>Distributed infrastructure</b> Cloud and edge computing
 <b>4</b> <b>Next-generation computing</b> Quantum computing Neuromorphic chips (ASICs <sup>4</sup> )	 <b>5</b> <b>Applied AI</b> Computer vision, natural-language processing, and speech technology	 <b>6</b> <b>Future of programming</b> Software 2.0	 <b>7</b> <b>Trust architecture</b> Zero-trust security Blockchain

Industry-specific trends

 <b>8</b> <b>Bio Revolution</b> Biomolecules <sup>5</sup> -omics <sup>6</sup> / biosystems Biomachines/biocomputing/augmentation	 <b>9</b> <b>Next-generation materials</b> Nanomaterials, graphene and 2-D materials, molybdenum disulfide nanoparticles	 <b>10</b> <b>Future of clean technologies</b> Nuclear fusion Smart distribution/metering Battery/battery storage Carbon-neutral energy generation
--	---	---

# Latest Technology Trend





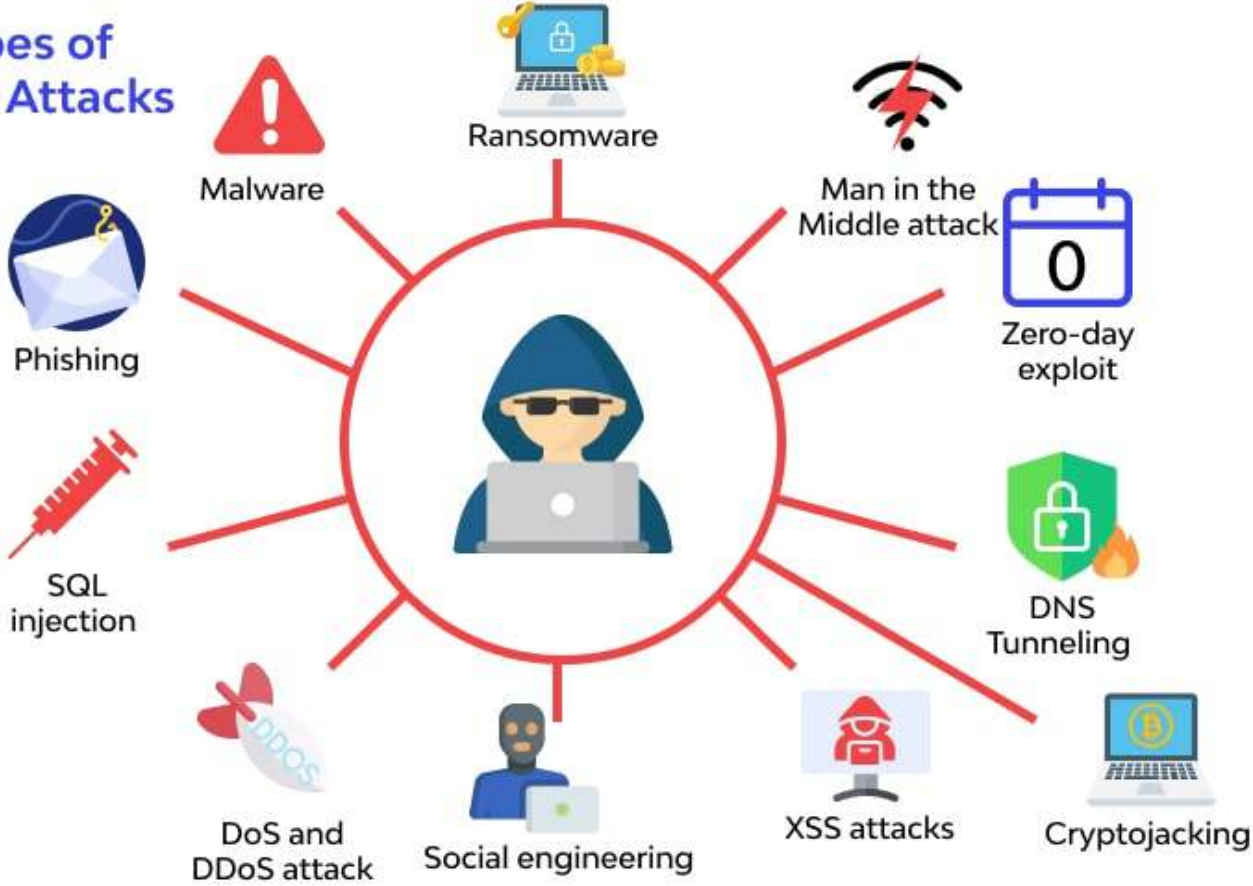
*Cyber Attack*





# Cyber Attack: Increasing Trend & Variety

## Types of Cyber Attacks





# Cyber Attack: Case Study & Statistics



## Cyber Attack: Case Study & Statistics



**IDN TIMES**

### Dampak Serangan Siber ke Perbankan RI

- Kerugian ekonomi hingga Rp14,2 triliun\*
- Menggerus kepercayaan publik terhadap sistem perbankan dan ekonomi secara keseluruhan
- Kebocoran data nasabah
- Hilangnya data nasabah
- Mengganggu stabilitas sosial dan politik

The infographic features a blue background with a grid pattern. In the top right corner, the 'IDN TIMES' logo is displayed in white and red. The title 'Dampak Serangan Siber ke Perbankan RI' is written in large, bold, dark blue letters. Below the title, five bullet points are listed, each with a white dot and text in white on a dark blue rectangular background. At the bottom right, there is a stylized illustration of a person wearing a black hijab and a pink face mask, with a bar chart and data points in the background.

## Cyber Attack: Case Study & Statistics

**D**katadata.co.id

Keuangan | OJK: Serangan Siber Rugikan Bank Rp 246,5 Miliar

### OJK: Serangan Siber Rugikan Bank Rp 246,5 Miliar, Mayoritas Bank BUMN

Sebanyak 71,6% serangan ditujukan kepada bank BUMN. Kemudian, bank swasta 28%, dan sisanya 0,3% serangan dilakukan kepada bank asing.

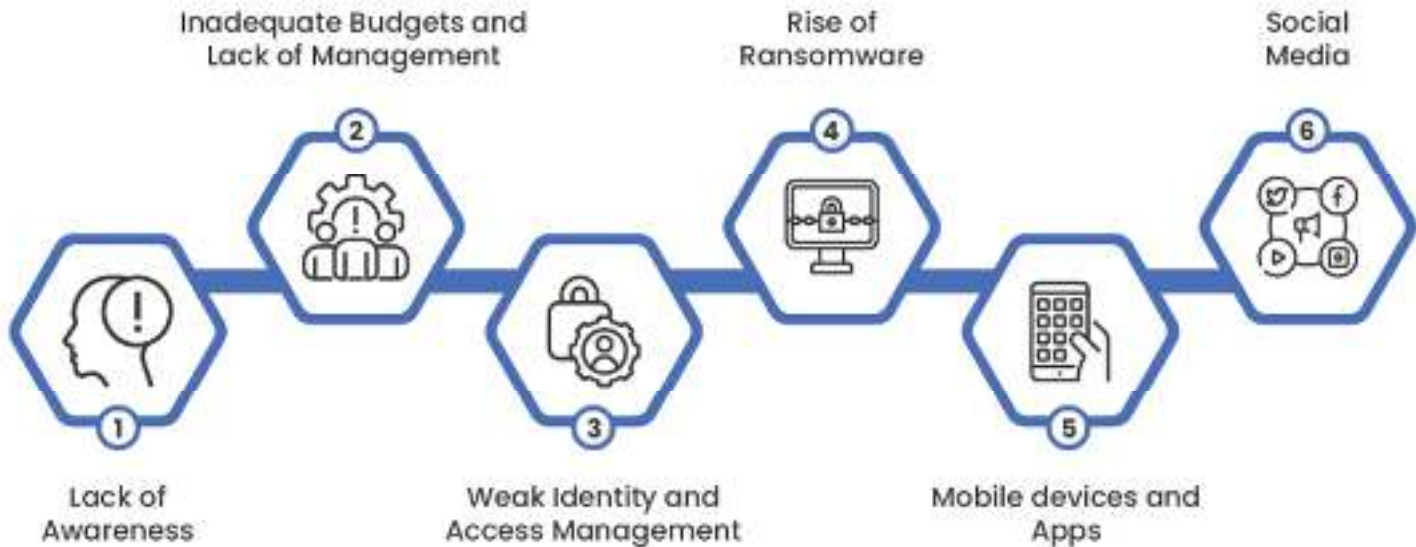


Oleh **Ihya Ulum Aldin**



26 Oktober 2021, 16:02

# Cyber Attack: Case Study & Statistics

## Challenges Related to Cybersecurity in the Banking Sector



<https://threatcop.com/blog/cybersecurity-in-banking>



*Banking, FinTech, Digital Wallet*

# Indonesia Strategic Direction

## 5 LANGKAH TRANSFORMASI DIGITAL NASIONAL



Sesuai Arahan Presiden pada 3 Agustus 2020



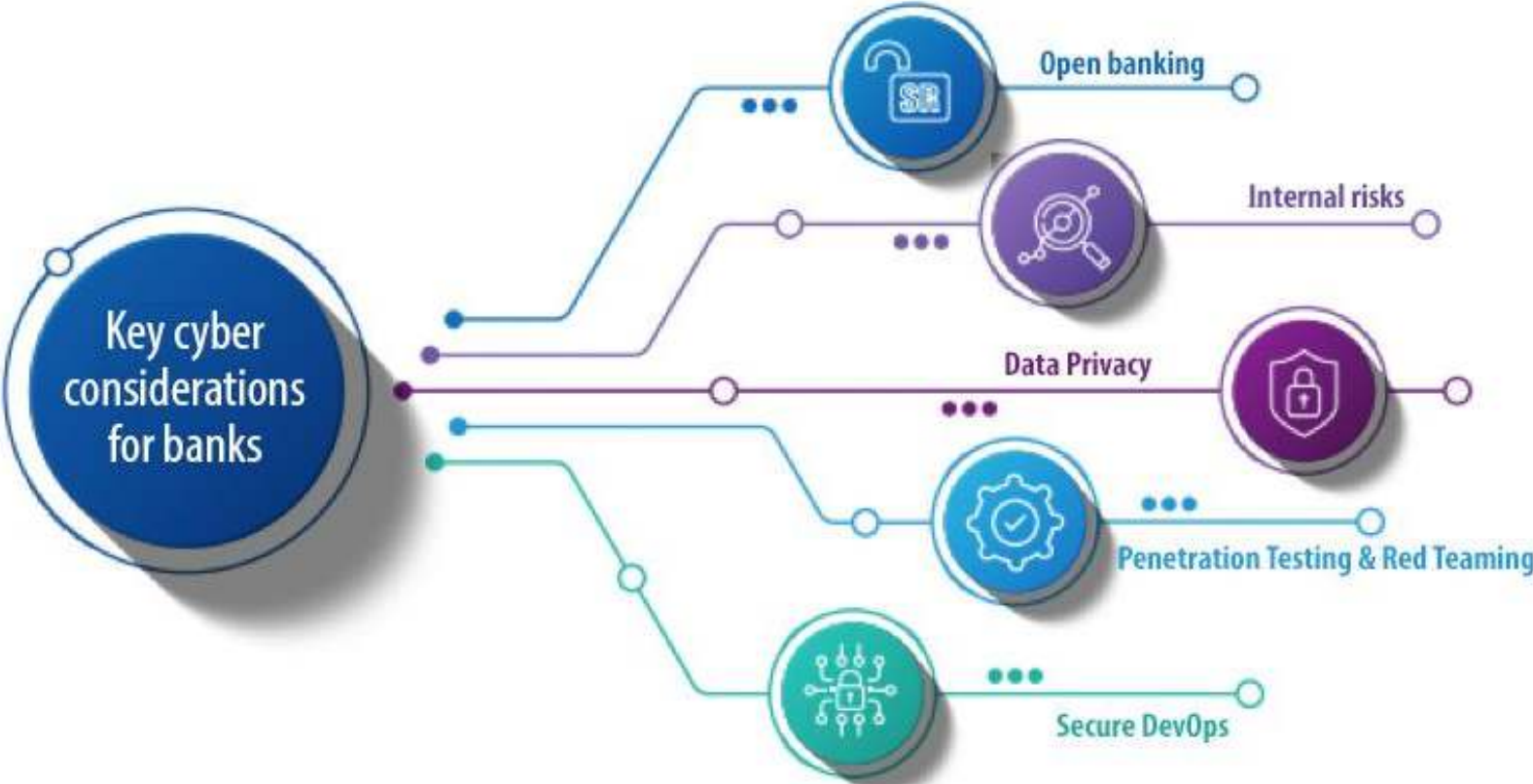


# Current Progress: Indonesia Banking Ecosystem





# Improving Digital Security in Banking & Payment



# Improving Digital Security in Banking & Payment



<https://intellipaat.com/blog/cyber-security-tips-best-practices>

# Improving Digital Security in Banking & Payment

## 1 BERSELANCAR DENGAN BIJAK



Hati-hati saat menyambungkan perangkat ke Wi-Fi publik yang tidak terjamin keamanannya. Selalu pakai kata sandi yang kuat dan unik di setiap akun. Aktifkan verifikasi dua langkah untuk lebih amannya.



## 2 JAGA PRIVASI

Ubah fitur kontrol keamanan dan privasi TikTok yang mudah digunakan untuk menyesuaikan pengalaman online kamu.



## 3 AWAS TERPANCING

Phising adalah taktik yang digunakan untuk mencuri informasi pribadi. Hindari membuka, mengunduh, atau mengklik tautan dan lampiran dari pengirim yang tidak dikenal.

## 4 JANGAN TINGGALKAN JEJAK

Perbarui semua perangkat dan aplikasi dengan versi terbaru dan hapus aplikasi yang tidak digunakan. Sebelum hendak menjual perangkat, pindahkan semua data pribadi, foto, atau video, lalu hapus semua konten di perangkat tersebut agar aman.



## 5 MAINKAN, TONTON, DAN PELAJARI BERSAMA



Unduh aplikasi, tonton video, mainkan game, dan tetap terhubung bersama keluarga. Pelajari lebih lanjut di Panduan Pengguna Baru kami.

# Improving Digital Security in Banking & Payment



## TIPS AMAN PAKAI PEMBAYARAN DIGITAL

**Perangkat & Internet Sendiri**  
Gunakan perangkat dan sambungan internet pribadi, menggunakan WiFi publik dapat berisiko penjahat siber meretas data Anda.

**Jaga Kerahasiaan PIN**  
Simpan nomor PIN, kata sandi dan kode one-time password (OTP) untuk diri sendiri. Jangan membagikan kode atau kata sandi ke orang lain.

**Waspada Akun Palsu**  
Waspada komunikasi di dunia digital yang mengatasnamakan akun-akun terpercaya. Jangan pernah memberikan informasi pribadi di dunia maya.



**Thank You!**