



# ANTISIPASI KEAMANAN DAN KESELAMATAN DIGITAL

Tim Literasi Digital Sektor Pemerintahan  
Kemenkominfo RI  
2023



# CV. Pemateri



# HASIL BELAJAR

Peserta mampu menjelaskan antisipasi keamanan dan keselamatan digital di sektor pemerintahan

## INDIKATOR HASIL BELAJAR

Setelah mengikuti materi ini peserta mampu menjelaskan :

1. Dampak (positif & negatif) digitalisasi
2. Manajemen risiko digitalisasi

# Dampak Positif Digitalisasi

- Meningkatkan kualitas hidup Individu dan Masyarakat
- Mempermudah penyimpanan & penyediaan data, kecepatan perolehan data, kelengkapan data,
- Kemudahan komunikasi, kemudahan dan kecepatan layanan publik, kemudahan bisnis, layanan kesehatan, bisnis logistik, dll.



# Dampak Positif Digitalisasi

1. **Efisiensi:** Digitalisasi mempermudah akses dan pengolahan informasi, sehingga membuat proses bisnis lebih cepat dan efisien.
2. **Pertumbuhan Ekonomi:** Digitalisasi membuka peluang baru bagi bisnis dan industri, yang pada gilirannya membantu meningkatkan pertumbuhan ekonomi.
3. **Aksesibilitas:** Digitalisasi membuat informasi dan layanan lebih mudah diakses oleh masyarakat, terutama bagi mereka yang berada di daerah terpencil

# Dampak Positif Digitalisasi

**4. Kemudahan Komunikasi:** Digitalisasi mempermudah komunikasi antar individu atau antar organisasi, baik secara lokal maupun internasional.

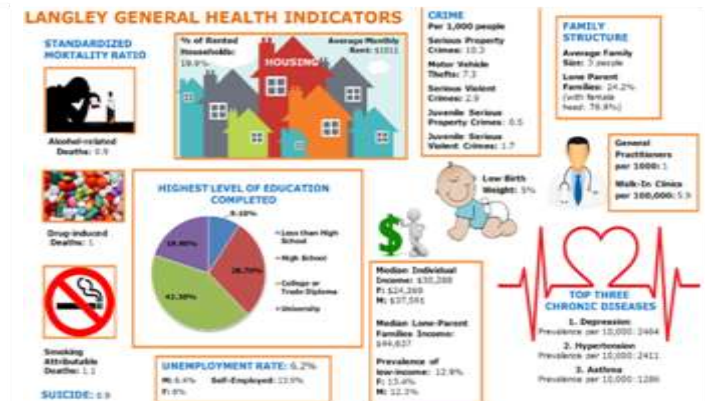
**5. Inovasi:** Digitalisasi mendorong inovasi dalam bidang teknologi dan bisnis, sehingga membantu memecahkan masalah dan memenuhi kebutuhan masyarakat.

**6. Edukasi:** Digitalisasi membuat akses terhadap sumber belajar dan informasi menjadi lebih mudah dan luas yang pada





# Dampak Positif Digitalisasi





# Dampak Positif Digitalisasi



GoodStats

## Daftar Terbaru Decacorn dan Unicorn Indonesia

Per Agustus 2022

DECACORN		
Valuation \$ Billion Dolar AS (Miliar)	 Go Far, Go Together	 Express Your Online Business
	Sudah IPO	\$20B
UNICORN		
		
Sudah IPO	\$3B	\$2,9B
		
\$2B	\$1,3B	\$1B
		
\$1B	\$1B	\$1B

www.goodstats.id  
@goodstats.id

Sumber: CB Insight



# Dampak Negatif Digitalisasi

- Mengganggu Kehidupan Individu dan Masyarakat
- Gangguan kerahasiaan, kebocoran data, akurasi data, komunikasi data, dll,
- Potensial berkembang mengganggu perekonomian, kenyamanan hidup, perpecahan bangsa, keamanan suatu negara, dll.

# Dampak Negatif Digitalisasi

1. **Kerugian pekerjaan:** Beberapa jenis pekerjaan dapat terancam oleh otomatisasi dan digitalisasi, sehingga menyebabkan pengangguran dan kerugian pendapatan bagi banyak orang.
2. **Isolasi sosial:** Terlalu banyak terlibat dalam dunia digital dapat mengurangi interaksi sosial dan kualitas hubungan antar individu.
3. **Cybercrime:** Digitalisasi juga membuka peluang bagi tindak kejahatan seperti peretasan, pencurian identitas, dan phishing, yang dapat merugikan individu dan bisnis.
4. **Ketergantungan:** Masyarakat dapat terlalu tergantung pada teknologi digital, yang dapat mempengaruhi keterampilan dan kemampuan mereka untuk berfungsi tanpa teknologi.
5. **Kekurangan privasi:** Digitalisasi mempermudah penyimpanan dan pengolahan data pribadi, yang dapat menimbulkan risiko privasi dan keamanan informasi.



**BerAKHLAK**  
Berorientasi Pelayanan, Akuntabel, Kompeten,  
Harmonis, Berkeadilan

#bangga  
melayani  
bangsa

MAKIN  
CAKAP  
DIGITAL

# Dampak Negatif Digitalisasi





# Dampak Negatif Digitalisasi



# Tantangan Terbesar Risiko Individu

- Terjebak menjadi penyebar Hoax dan Peserta Proxy War
- Melakukan kesalahan karena tidak paham dampak risikonya
- Melanggar rambu2 Peraturan karena tidak paham manfaat rambu2 aturan yang dibuat
- Melakukan penyimpangan IT Governance dalam menjalankan tugas sebagai Aparatur Pemerintahan
- Terjebak risiko individu akibat :
  - Melakukan tindakan pribadi tanpa pertimbangan risiko akibat penyimpangan rambu2 yang berlaku
  - ketidak pastian hukum selama masa tranformasi digital

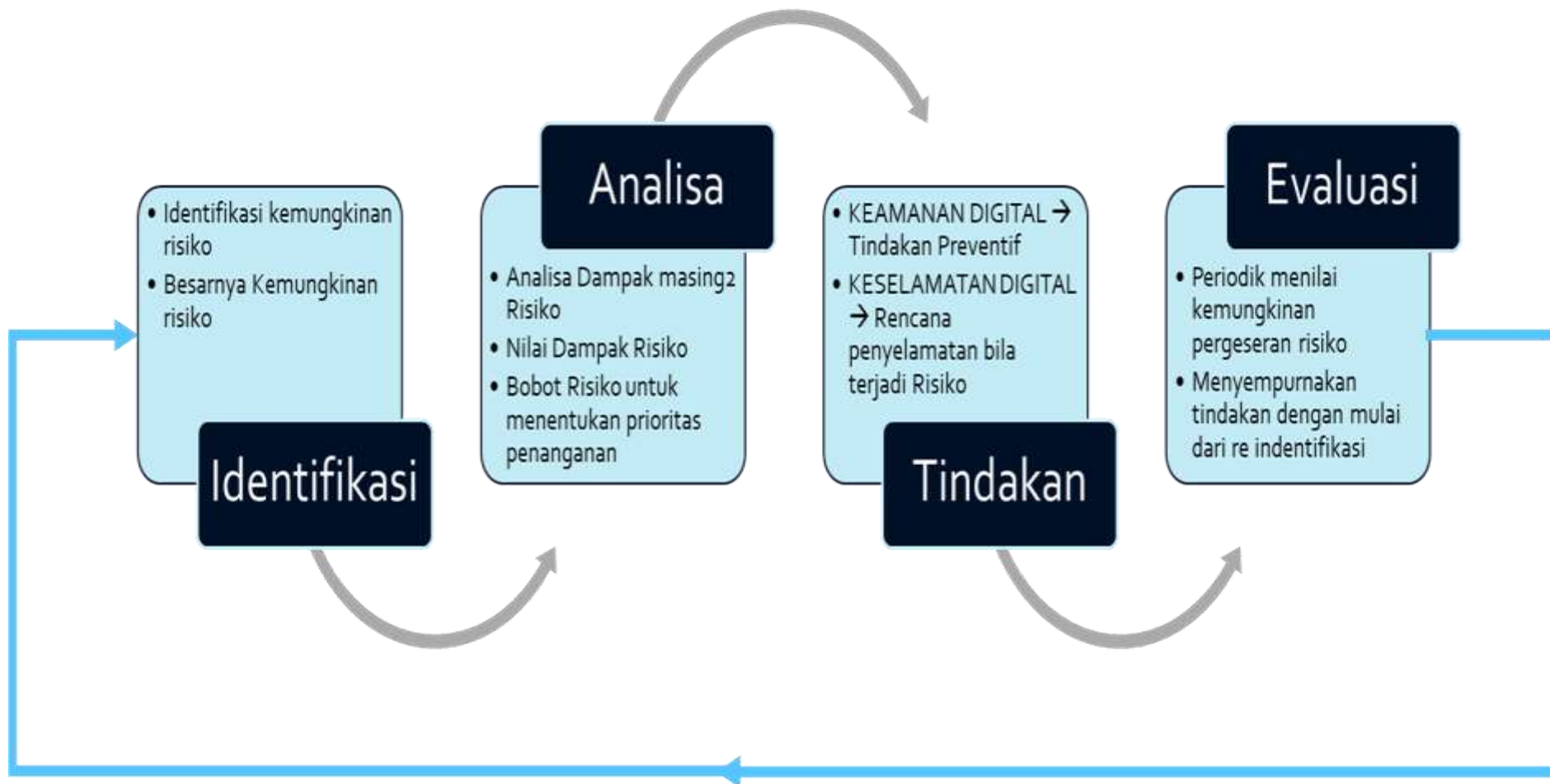




# Manajemen Risiko bagi Keamanan & Keselamatan Digital

- Perlu dilaksanakan oleh Penyelenggara Negara, Penyelenggara Proses Digitalisasi, maupun Individu pengguna fasilitas digital.
- Ditujukan untuk memahami risiko yang perlu diantisipasi oleh masing2 pihak untuk diamankan tanpa mengurangi manfaat maupun mempersiapkan penyelamatan apabila risiko terjadi
- Manajemen Risiko Penyelenggara Negara menghasilkan rambu2 Peraturan dan Perundangan yang berlaku untuk dilaksanakan agar kehidupan digital terjamin aman dan minim risiko
- Manajemen Risiko Penyelenggara Proses Digital menghasilkan rambu2 Tatakelola Proses Digital sebagai bentuk terapan IT Governance untuk menjamin agar proses digital terjamin aman dan minim risiko

# TAHAPAN MANAJEMEN RISIKO SEDERHANA



# Keamanan Umum dan Pemerintahan

- Ada 3 upaya tindakan Preventif Keamanan Digital Umum dan Kegiatan Pemerintahan:
  - Kepatuhan terhadap Peraturan dan Perundangan terkait dengan digitalisasi
  - Kepatuhan pelaksanaan tugas sesuai Aturan Tatakelola masing2 bidang.
  - Antisipasi tindak preventif sesuai hasil analisa dalam manajemen risiko individual
- Untuk Pengamanan Sistem Pemerintahan :
  - Tersedia Peraturan Perundangan berikut standar dan tatakelola yang berlaku untuk memperkecil risiko digitalisasi Pemerintahan bila dipatuhi
  - Ketidakpatuhan akan berdampak sebagai risiko individu, kecuali bila SOP/Prosedur unit kerja yang diperlukan sebagai turunan kebijakan dibuat bertentangan dengan peraturan di atasnya dan akan menjadi risiko jabatan bagi pimpinan

# Melaksanakan Keamanan dan Keselamatan secara Individu

- Menjalankan Prinsip Keamanan mulai dari ring terluar:
- Pengamanan Fisik sarana digital: HP, Komputer, Kartu, Kunci/password/Pin, Kartu Identitas dll.
- Pengamanan Software: Baca dulu sebelum setuju, jangan sembarang pasang program, review dan bersihkan histori penggunaan/anti virus/program ilegal, dll.
- Pengamanan Data: Jangan simpan terlalu banyak di HP/Komputer, backup dan pasang password, simpan backup ditempat aman dll.
- Melaksanakan Prosedur Keselamatan dan Mempelajari Prosedur Keadaan darurat sehingga bila risiko terjadi akan meminimalisasi dampak yang dihadapi.

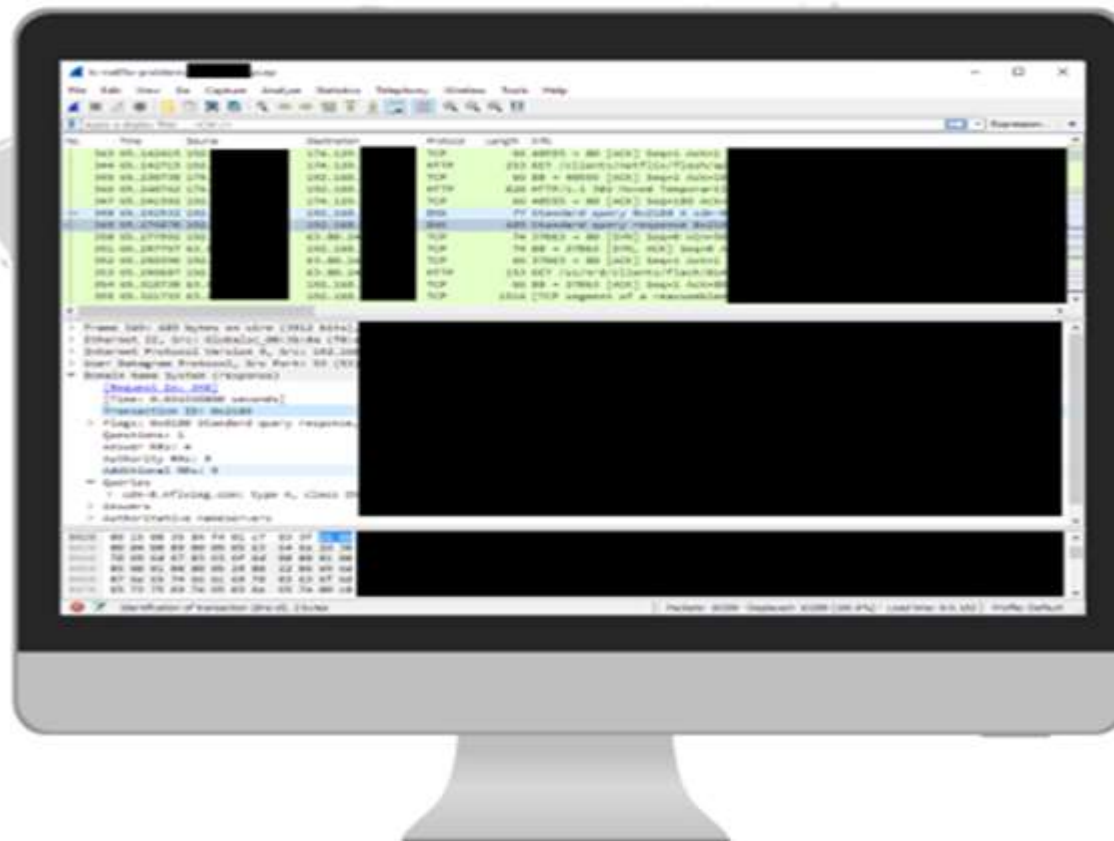
# Tips Melindung Data Pribadi

1. Gunakan Password yang kuat (Kombinasi huruf kapital-Non Kapital, angka, karakter)
2. Pastikan pengaturan privasi di tiap akunnya sesuai dengan tingkat keamanan yang dibutuhkan
3. Hati-hati mengunggah data pribadi pada platform digital
4. Hindari membagikan data pribadi
5. Hindari membagikan data pribadi milik orang lain
6. Waspada saat menggunakan Wifi publik
7. Pastikan mengetahui fungsi dari aplikasi yang akan dipasang
8. Lakukan pembaruan perangkat lunak secara berkala
9. Waspada jika ada komunikasi atau aktivitas mencurigakan
10. Bedakan email pekerjaan dengan email pribadi

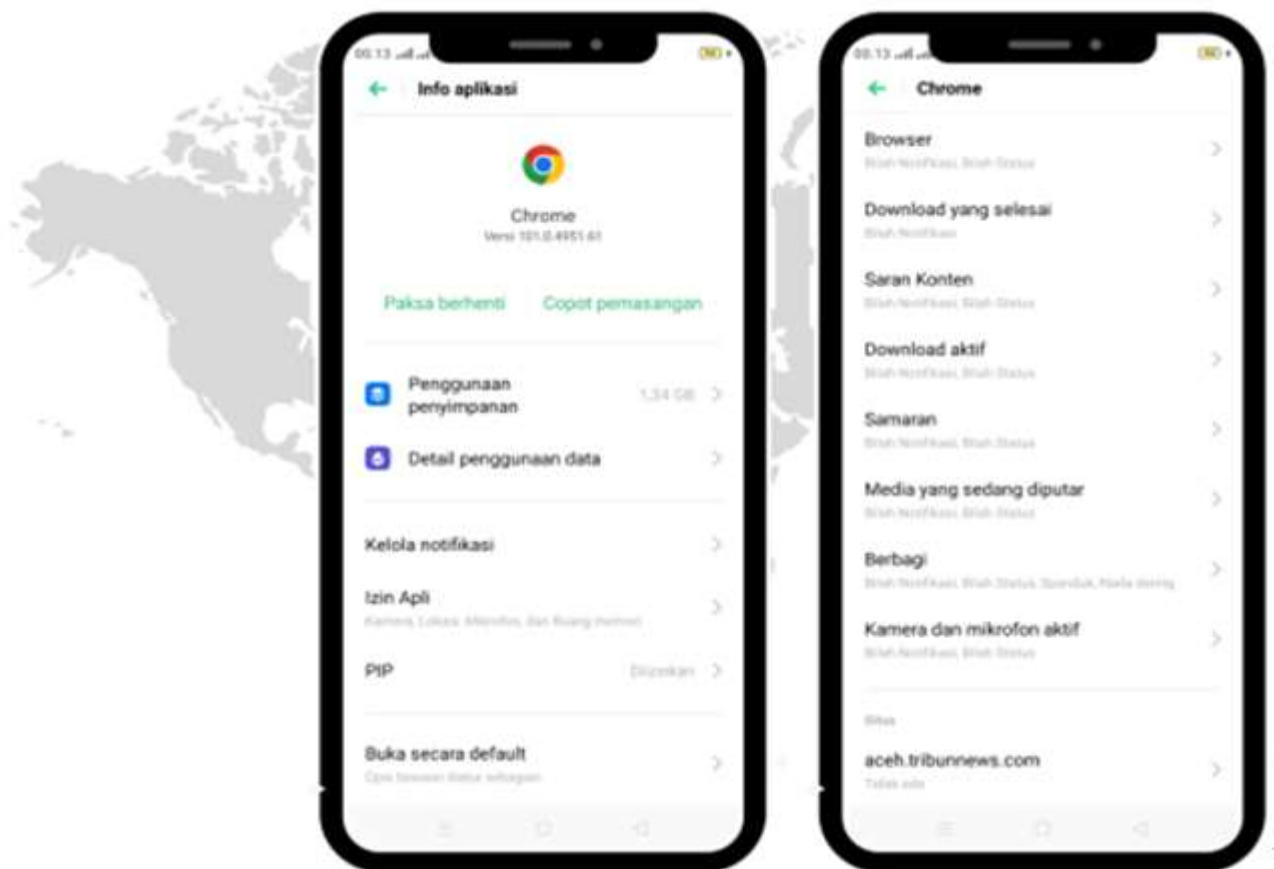




# Tips Perlindungan Data Pribadi: Waspada saat menggunakan wi-fi publik



# Tips Perlindungan Data Pribadi: Pastikan mengetahui fungsi dari aplikasi yang diinstall



# KESIMPULAN

- Dalam Keamanan Digital peran individu memahami manfaat dan risiko akan meningkatkan kewaspadaan masing2 individu agar tidak terjebak pada masalah yang tidak dipahami.
- Dalam hal tanggung jawab penataan keamanan dan keselamatan untuk hal yang perlu dilaksanakan bersama secara organisasi dan merupakan tanggung jawab Pimpinan:
  - Minimal harus melengkapi dengan standar dan prosedur internal.
  - Bila Induk organisasi yang berwenang tidak mengatur maka Pengguna Fasilitas wajib mengingatkan penanggung jawabnya
- Hindari tanggung jawab tugas yang (dibuat) tidak jelas dengan melakukan proteksi diri dengan melakukan



#MakinCakapDigital



# TERIMA KASIH