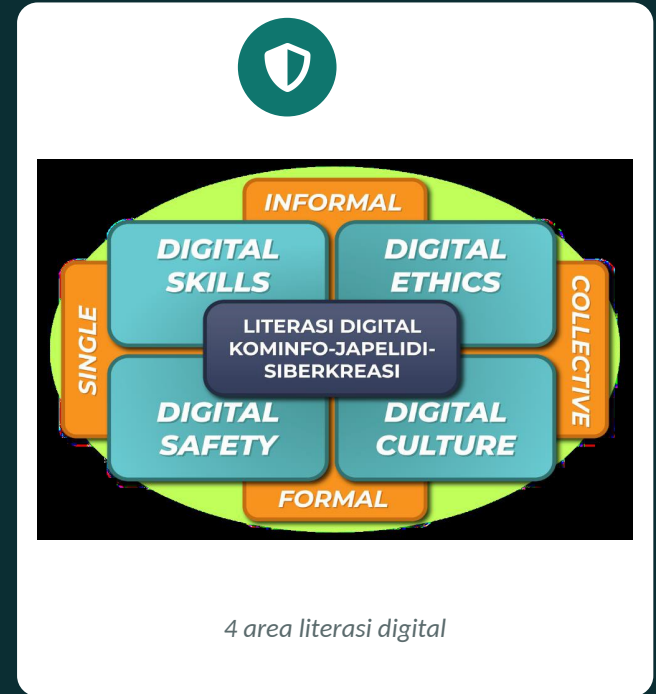


# Aman Bermedia Digital

Panduan lengkap melindungi perangkat, identitas, data pribadi, rekam jejak, dan anak di ruang digital



# Tujuh Bab, Satu Tujuan: Aman Bermedia



## Bab I

Aman diri & sesama di ruang digital



## Bab II

Memproteksi perangkat digital



## Bab III

Identitas digital & data pribadi



## Bab IV

Memahami & menghindari penipuan



## Bab V

Melindungi rekam jejak digital



## Bab VI

Keamanan anak di platform digital



## Bab VII

Tantangan keamanan digital

Tiap bab: urgensi, konsep, praktik, simulasi & evaluasi

# Hidup Serba Digital, Peluang & Risiko

**73,7%**

penetrasi internet Indonesia  
(APJII 2020)

**196,71  
jt**

penduduk Indonesia  
mengakses internet

**88%**

pengguna internet >15 th  
berbelanja daring (2019)

**Rp621 T**

total transaksi digital 2020, naik  
11% (Google & Temasek)

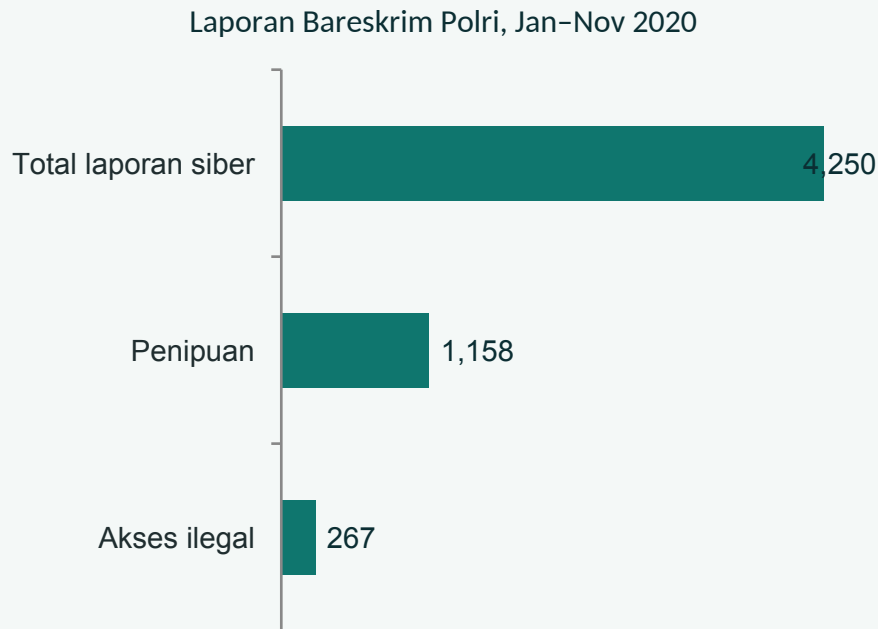
## Peluang

- Belanja, bekerja, sekolah, dan layanan publik cukup lewat gawai
- Membandingkan harga, negosiasi, hingga transaksi keuangan dalam sekejap
- Masyarakat lebih berdaya dan nyaman bertransaksi digital

## Risiko

- Celah pencurian data terbesar ada pada sisi pengguna
- Penipuan dan pencurian akun terus terjadi di berbagai platform
- Fitur 2FA dan ajakan ganti sandi belum cukup tanpa kewaspadaan

# Kejahatan Siber di Indonesia



Gambar I.1 — Jumlah kasus kejahatan siber (Bareskrim, CNN 2020)

Keamanan akun hanya satu sisi. Spektrum keamanan digital jauh lebih luas: perangkat, identitas, penipuan, rekam jejak, hingga keselamatan anak.

# Apa Itu Keamanan Digital?

*Proses memastikan penggunaan layanan digital, daring maupun luring, dapat dilakukan secara aman dan nyaman — melindungi data yang kita miliki sekaligus data pribadi yang bersifat rahasia.*



## Kontrol ada di pengguna

Penyedia layanan hanya menyediakan fasilitas pengaman. Pelaku lebih suka menipu pengguna yang lengah daripada meretas sistem penyedia layanan.



## Interaksi luas & anonim

Nama pengguna belum tentu identitas asli. Siapa pun bisa menjadi sosok berbeda, sehingga kita rentan berinteraksi dengan pihak yang niatnya tidak jelas.



## Ada pengguna rawan

Anak-anak dan lansia kurang matang secara psikis. Penggunaan internet yang intrusif bisa memengaruhi kesehatan mental, sehingga literasi lanjutan mutlak dibutuhkan.

# Kerangka Kompetensi Literasi Digital

Japelidi (2018)

10 kompetensi

Tular Nalar (2020)

8 kompetensi

BSSN (2020)

5 kompetensi

Kominfo, Siberkreasi & Deloitte (2020)

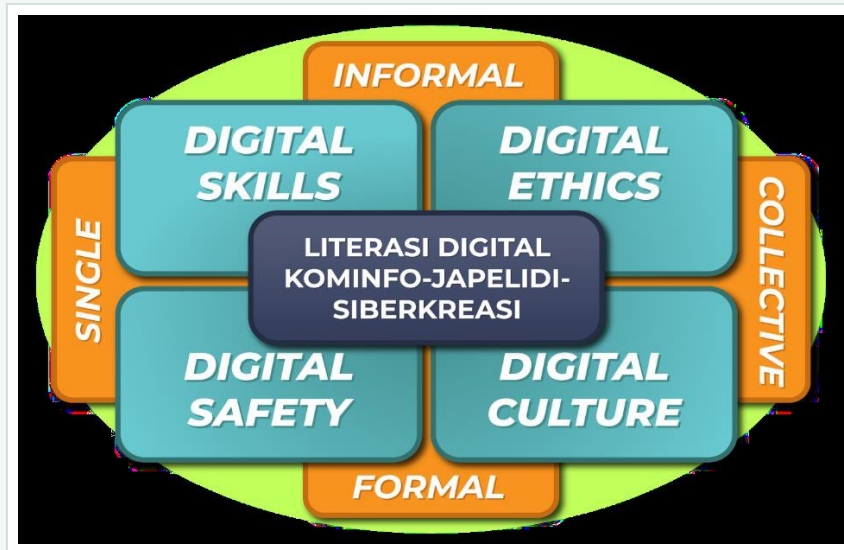
4 area kompetensi

## Fungsional

Akses, seleksi, paham, distribusi, produksi

## Kritis

Analisis, verifikasi, evaluasi, partisipasi, kolaborasi



4 area: Digital Skills, Culture, Ethics, Safety

# Peta Kompetensi Keamanan Digital



*Kompetensi fungsional ditekankan pada proteksi perangkat; empat lainnya membangun keterampilan fungsional sekaligus kritis.*

# Mengapa Perangkat Harus Dilindungi?



## Malware

Malicious software mengontrol perangkat diam-diam: mencuri sandi dan nomor akun, membebankan biaya palsu, melacak lokasi. Sering menyamar sebagai aplikasi "gratis" di luar toko resmi.

## Tertinggi

tingkat malware di Asia  
dipegang Indonesia (Microsoft  
2019)

60.000

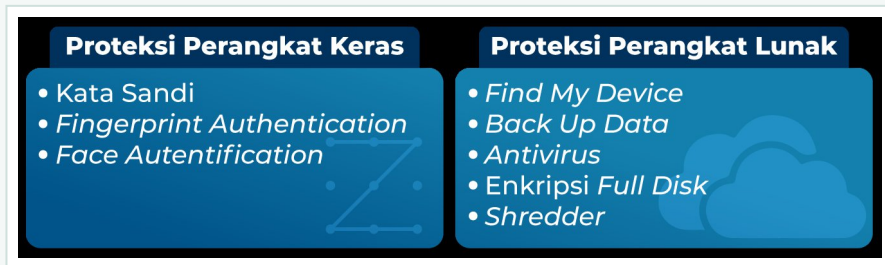
pesan penipuan bertema  
COVID-19 per hari, bermuatan  
tautan jahat



## Pelajaran dari kasus nyata

- Teknisi servis ponsel yang viral membuka galeri pelanggan untuk mencari foto dan video pribadi
- File yang "dihapus" sering masih bisa dipulihkan oleh orang yang paham teknologi
- Celah terbesar: pengguna lalai atau lupa mengaktifkan fitur pengaman

# Fitur Proteksi Perangkat Keras & Lunak



Bagan II.1 — Fitur proteksi perangkat keras (kiri) & lunak (kanan)



Bagan II.2 — Cara aman menggunakan kata sandi

Gunakan produk asli agar sistem terus diperbarui melawan malware baru.



## Kata sandi / pola

Kombinasi angka dan huruf; rahasiakan, tutup layar saat mengetik, dan ubah rutin.



## Sidik jari

Sulit ditiru meski orang melihat cara kita membuka; tidak semua perangkat mendukung.



## Pencocokan wajah

Aman terhadap foto wajah, tetapi wajah harus terbuka (kurang praktis bila bermasker/berkacamata).

## Lapisan Pengaman Ekstra (Opsional)



### Find My Device

Melacak & mengunci perangkat hilang. Remote wipe mengembalikan ke setelan pabrik dan menghapus semua data.



### Back-up Data

Cadangkan foto, dokumen, kontak ke Google Drive, OneDrive, iCloud. Pastikan terenkripsi dan sandi aman.



### Antivirus

Pilih produk bereputasi yang fokus pada perlindungan; konsultasikan ke teknisi terpercaya.



### Enkripsi Full Disk

Seluruh hard drive disandikan (mis. BitLocker). Fitur tingkat lanjut; konsultasikan dulu.



### Shredder

Memusnahkan data total sehingga tidak bisa dipulihkan, misalnya File Shredder.

*Fitur ini opsional: bila aktivitas kita tidak terlalu berisiko, perangkat tambahan tidak selalu dibutuhkan.*

# Sebelum Menjual atau Memindahtangankan

≈90%

perangkat bekas masih menyimpan data sensitif (Kaspersky)

Kesalahan umum: hanya menghapus atau format ulang. Cara ini cuma menyembunyikan data dari layar, masih bisa dikembalikan.

1

Cadangkan data dengan aman

2

Timpa (overwrite) penyimpanan agar tak bisa dipulihkan

3

Lepas SIM & kartu memori; hapus eSIM

4

Aktifkan 2FA pada akun penting

5

Log out dari bank, email, media sosial

6

Lakukan factory reset atau format media

*Ponsel layar pecah? Gunakan program VNC untuk mengambil data lewat komputer.*

# Tujuh Rekomendasi Proteksi Perangkat

1

Beli perangkat di agen resmi

2

Cek kode perangkat di kemasan dengan yang tertera pada perangkat

3

Biasakan membaca buku panduan pemilik

4

Pilih kata sandi paling aman yang mudah diingat

5

Jangan mudah memperlihatkan atau meminjamkan perangkat tanpa pengawasan

6

Waspada tawaran situs daring yang menggiurkan

7

Sterilkan perangkat sebelum diganti dengan yang baru

*Tanggung jawab dibagi: individu, pelaku pasar perangkat, dan negara (kebijakan yang adil & berbasis HAM).*

# Kasus Kebocoran Data yang Mengguncang

**87 juta**

data pengguna Facebook bocor — skandal Cambridge Analytica

**US\$5 M**

denda FTC untuk Facebook ( $\approx$  Rp70 triliun), terbesar sepanjang sejarah FTC

**91 juta**

data pengguna Tokopedia diduga bocor (Juli 2020)



**Zoom, April 2020**

530.000 data sandi dan detail akun bocor. Bukan dari aplikasinya, melainkan karena sandi yang sama dengan sandi email pengguna diretas.



**Big data, risiko besar**

Data pengguna yang terkumpul masif membuka peluang bocor saat disimpan maupun diproses. Indonesia belum memiliki regulasi perlindungan data pribadi yang menjamin hak warga.

# Memahami & Melindungi Identitas Digital

## Apa itu identitas digital?

Identitas seseorang sebagai pengguna platform digital; gabungan identitas parsial. Bisa sama atau berbeda dengan dunia nyata, dan satu orang dapat punya banyak persona.

### Identitas tetap

Nama, tempat & tanggal lahir, jenis kelamin, nama orang tua (tercatat di KK/KTP)

### Identitas tidak tetap

Pekerjaan, alamat tinggal, penampilan fisik yang bisa cepat berubah

#### Identitas yang Terlihat

- Nama akun
- Foto profil pengguna
- Deskripsi pengguna
- Identitas lain yang tercantum dalam akun

#### Identitas yang Tidak Terlihat

- PIN/Password/Sandi
- *Two Factor Authentication*
- OTP
- Identitas lain

Bagan III.1 — Jenis identitas digital

1.

Pastikan memilih menggunakan identitas asli atau samaran saat mengelola akun platform digital serta bertanggungjawab atas pilihan tersebut

2.

Amankan identitas utama yakni alamat surat elektronik (surel) yang kita gunakan untuk mendaftar suatu platform digital

3.

Lindungi dan konsolidasikan identitas digital dalam berbagai platform digital yang dimiliki

Bagan III.2 — Tiga langkah melindungi identitas digital

# Memahami & Melindungi Data Pribadi

## Definisi

Data berupa identitas, kode, simbol, huruf atau angka penanda personal yang bersifat pribadi. Menurut GDPR (UE, 2016): segala informasi yang dapat digunakan untuk mengenali seseorang.



Email



Alamat IP



No. telepon



Data lokasi

*Privasi = hak memilih apakah data pribadi kita boleh diketahui pihak lain atau tidak.*

### Data Pribadi Umum

Nama, jenis kelamin, kewarganegaraan, agama, tanggal lahir, pekerjaan, alamat rumah, e-mail, nomor telepon, dan lainnya

### Data Pribadi Khusus

Data kesehatan, biometrik genetika, keuangan, ras/etnis, preferensi seksual, pandangan politik, data keluarga, data kejahatan dan lainnya

Bagan III.3 — Jenis data pribadi: umum & khusus

### TIPS PERLINDUNGAN DATA PRIBADI

Gunakan password (sand) yang kuat, gunakan secara berbeda di setiap akun platform digital yang dimiliki, dan perbaharui secara berkala

Pahami dan pastikan pengaturan privasi di setiap akun platform digital yang dimiliki sesuai dengan tingkat keamanan yang dibutuhkan

Hati-hati mengunggah data pribadi di platform digital karena keamanan data pribadi kita tidak selalu terjamin

Hindari untuk membagikan data pribadi kita (tempat tanggal lahir, nama ibu kandung, password berbagai akun platform digital)

Hindari berbagi data pribadi orang lain baik keluarga, teman, maupun kenalan di dunia maya sebab data mereka adalah privasi mereka

Hindari memasukkan data pribadi yang penting saat berinteraksi dalam platform digital dengan menggunakan Wi-Fi gratis di tempat publik

Pahami dan pilih aplikasi yang dipasang di gawai hanya mengakses data yang dibutuhkan dan bukan data pribadi kita lainnya

Selalu lakukan pembaruan perangkat lunak yang digunakan dalam gawai untuk meminimalisir resiko ada celah kebocoran

Waspada jika ada komunikasi atau aktivitas mencurigakan baik dari akun dengan identitas digital yang kita kenal maupun bukan

Bagan III.4 — Tips perlindungan data pribadi

# Tiga Gembok Digital



## PIN

*Personal Identification Number*

- Angka sandi 4–6 digit yang hanya diketahui pengguna & sistem
- Hindari tanggal lahir / kombinasi mudah ditebak
- Jangan tulis di KTP atau kertas di dompet
- Beda PIN untuk keperluan berbeda
- Tutup tangan saat mengetik di ATM



## 2FA

*Two-Factor Authentication*

- Butuh dua faktor identifikasi: sandi + faktor lain
- Faktor lain: kode SMS, persetujuan di ponsel, sidik jari
- Sangat menekan peluang akun dibajak
- Tetap tidak 100% aman; jaga nomor ponsel



## OTP

*One-Time Password*

- Kode unik 6–8 digit, sekali pakai per transaksi
- Dikirim lewat SMS atau email
- Salah satu angka saja, transaksi gagal
- Jangan pernah diberikan kepada siapa pun

# Melindungi Data Saat Bertransaksi Daring



Poster "BERSAMA Jaga Data Pribadi"



## Verifikasi platform

Bandingkan keamanan platform dengan platform jual beli lain.



## Verifikasi akun lawan transaksi

Cek penjual maupun pembeli sebelum bertransaksi.



## Gunakan fitur pembayaran platform

Hindari rekening pribadi untuk mencegah penyalahgunaan data.



## Hargai data orang lain

Jangan sebar data pribadi orang lain (mis. pasien COVID-19); dilindungi hukum.

Dasar hukum: UU ITE Pasal 26, PP 71/2019 (PSTE), PM Kominfo 20/2016.

# Penipuan Digital: Ancaman Nomor Dua

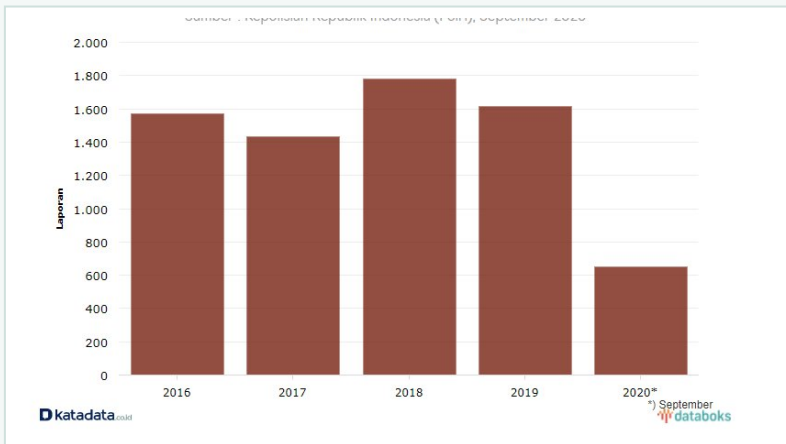
**95,4%**

pengguna internet  
mengakses lewat  
smartphone

**7.047**

kasus penipuan daring  
dilaporkan 2016–Sep 2020

**Kompetensi kunci: analisis,  
verifikasi, evaluasi**



Gambar IV.1 — Laporan penipuan daring per tahun (Polri)

**649 dari 2.259**

laporan kejahatan digital Jan–Sep  
2020 adalah penipuan daring,  
peringkat kedua terbanyak. Banyak  
korban tak melapor.

Sasaran utama: belanja daring di lokapasar seperti Shopee, Tokopedia, Bukalapak, dan Lazada. Modus: barang tak sesuai / tak dikirim, transfer fiktif, hingga pencurian data.

# Empat Bentuk Penipuan Digital



## SCAM

Memanfaatkan empati & kelengahan lewat telepon, SMS, WhatsApp, email. Contoh: Nigerian scam, romance scam (profile cloning), minta PIN/OTP.



## SPAM

Pesan bertubi-tubi tanpa diminta: iklan, email berisi tautan berbahaya, telepon dan SMS hadiah palsu.



## PHISHING

Menduplikasi situs/aplikasi bank atau provider untuk mencuri data sensitif. Varian: vishing (suara), smishing (SMS).



## HACKING

Mencari dan menembus kelemahan sistem komputer. Bila disalahgunakan menjadi kejahatan siber (mis. peretasan akun & situs).

# Mengenali & Mengendalikan Scam dan Spam



Waspada penipuan online shop via medsos

## Tips hindari scam

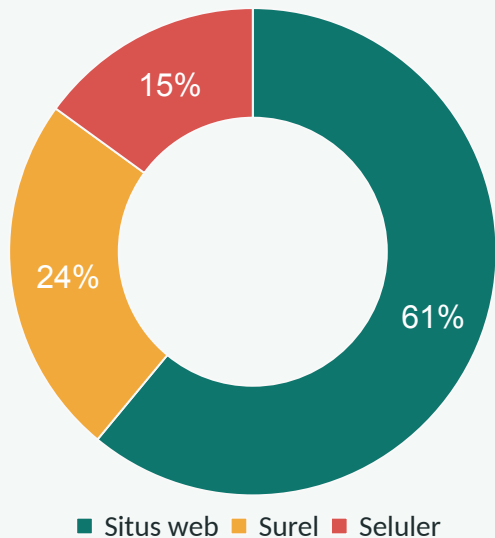
- Jaga identitas pribadi
- Jangan beri PIN/OTP kepada siapa pun
- Cek kewajaran harga, jangan tergiur diskon besar
- Selektif memilih aplikasi transaksi
- Verifikasi penjual sebelum transfer

## Tips hindari spam

- Jangan klik tautan pada email/SMS tak dikenal
- Blokir nomor dan pengirim spam
- Laporkan SMS spam ke BRTI
- Waspada nomor asing: telemarketing, penagih, penipuan

# Phishing: Jebakan Situs & Pesan Palsu

Serangan phishing Q2 2020 (Check Point)



*Situs web mendominasi serangan phishing*

## Cara kerja

Pelaku menyamar sebagai lembaga sah, membuat situs mirip halaman bank lengkap dengan kolom ID dan sandi. Data yang dimasukkan korban direkam pelaku, lalu dipakai menguras rekening.

## Ciri & cara menghindari

- Ada permintaan sandi, login, data kartu, atau PIN
- Periksa alamat situs & pengirim sebelum mengisi data
- Bank tidak meminta data rahasia lewat telepon/SMS
- Gunakan perangkat lunak pendeteksi phishing

# Sanksi Hukum Penipuan Digital



## Hacking

Hacker yang menemukan kelemahan lalu melapor ke administrator bersifat positif. Bila dimanfaatkan untuk merugikan, itu kejahatan siber (contoh: peretasan data Tokopedia, situs KPU Yogyakarta).

### Regulasi terkait

- UU 11/2008 jo. UU 19/2016 (ITE)
- UU 8/1999 Perlindungan Konsumen
- UU 7/2014 tentang Perdagangan



### UU ITE Pasal 28 ayat 1 & 45A ayat 1

Berita bohong yang merugikan konsumen

**Penjara maks. 6 tahun dan/atau denda maks. Rp1 miliar**



### UU ITE Pasal 35 jo. 51 ayat 1

Manipulasi informasi agar tampak otentik (phishing)

**Penjara maks. 12 tahun dan/atau denda maks. Rp12 miliar**



### UU TPPU No. 8/2010 • UU Transfer Dana • KUHP 378

Pencucian uang, transfer dana, penipuan

**Ancaman penjara hingga 5 tahun; 6–20 tahun sesuai pasal**

# Menjadi Korban? Segera Laporkan!

1

**patrolisiber.id**

Laporan kejahatan siber ke Polri

2

**@aduanBRTI (DM Twitter)**

SMS spam: kirim tangkapan layar + nomor

3

**cekrekening.id • kredibel.co.id**

Cek & laporkan rekening penipu agar dibekukan

4

**OJK 1-500-655**

Pengaduan layanan keuangan; email konsumen@ojk.go.id

5

**lapor.go.id • SMS 1708**

Aduan lewat portal & aplikasi LAPOR!

6

**CS platform & bank**

Shopee, Tokopedia, Bukalapak, atau bank Anda



Alur kerja LAPOR!

# Apa Saja Jejak Digital yang Kita Tinggalkan?



*Jejak digital: pencarian, media sosial, lokasi, transaksi, dan lainnya*

**Cek jejakmu: ketik namamu di mesin pencari.**



## Jejak pasif

Tertinggal tanpa disadari: alamat IP, lokasi, riwayat penelusuran, cookie. Dipakai untuk profil pelanggan dan target iklan, bahkan dijual ke pihak lain.



## Jejak aktif

Sengaja kita bagikan: email, unggahan media sosial, komentar, formulir daring. Bisa memengaruhi peluang kerja dan reputasi.

# Sulit Dihapus, Maka Kelola dengan Bijak

## Sisi negatif

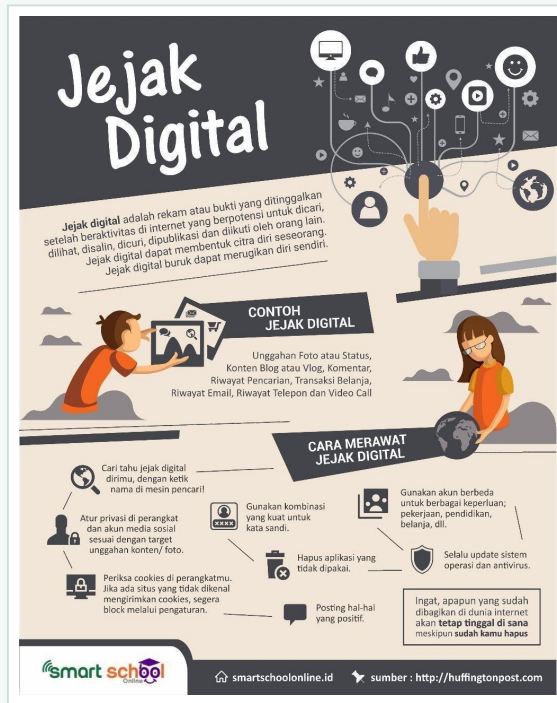
- Perundungan & doxing
- Pemerasan, revenge porn
- Kerusakan reputasi
- Data jadi komoditas

## Sisi positif

- Membantu aparat mengungkap kejahatan
- Portofolio karya & prestasi
- Nama baik saat dicari orang

## Cara melindungi jejak digital

- Baca syarat & ketentuan; tolak berbagi ke pihak ketiga bila ada pilihan
- Batasi data yang dibagikan; jangan unggah KTP, SIM, paspor, PIN
- Pikir sebelum mengunggah: "Jarimu harimaumu"
- Terapkan 10 kompetensi Japelidi: seleksi, verifikasi, evaluasi



*Jejak digital sulit hilang selamanya*

# Mengapa Keamanan Digital Anak Penting?

**92,82%**

pengguna internet di Indonesia  
memakai media sosial (2017)



## Pembuat pesan

Semua orang bisa membuat pesan; anak ingin punya akun & berinteraksi dengan orang asing



## Sifat pesan

Datang dari seluruh dunia tanpa saring, bisa bertentangan dengan nilai keluarga

**97,4%**

di antaranya generasi milenial



## Penyebaran pesan

Platform dirancang semenarik mungkin demi keuntungan ekonomi



## Dampak pesan

Sumber ilmu tak terbatas, namun juga hoaks, kekerasan, pornografi

Anak (0–18 tahun) belum sepenuhnya punya keterampilan berpikir kritis, sehingga paling berisiko terpapar dampak negatif media digital.

# Tujuh Ancaman bagi Anak di Dunia Digital



1. Perundungan



2. Eksploitasi & perdagangan orang



3. Pencurian data pribadi



4. Pelecehan seksual & pornografi



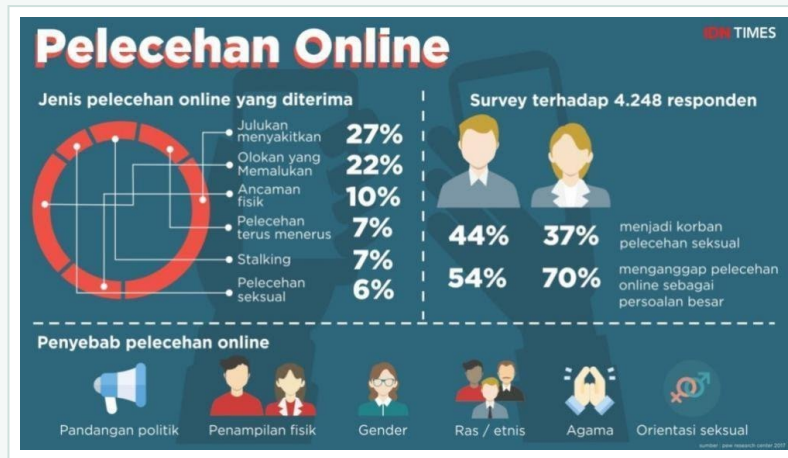
5. Penipuan



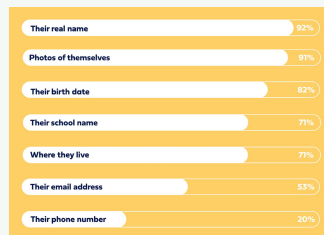
6. Kekerasan



7. Kecanduan gawai (nomofobia)



Infografis pelecehan online



Anak mudah membagikan data pribadi, bahkan kepada orang yang baru dikenal.

# Mendampingi Anak Bermedia Digital



## Kreativitas

Kenalkan olah kata, suara, angka, gambar, dan berbagai bentuk media digital



## Kolaborasi

Latih berkomunikasi, bernegosiasi, menghargai pendapat, membagi tugas



## Berpikir kritis

Tanamkan nilai keluarga agar anak kritis memilah pesan global

### Langkah praktis

- Diet gawai: batasi waktu layar, alihkan ke kegiatan nyata
- Pilih media sosial sesuai usia, dampingi sejak awal
- Blokir konten tak layak; ajari anak berani melapor



*Saring sebelum sharing*

# Lima Tantangan ke Depan



## Fitur & ancaman terus berkembang

Tetap waspada isu keamanan meski perangkat asli selalu diperbarui.



## Identitas & data makin kompleks

Kecerobohan kecil pengguna tetap jadi celah utama peretas.



## Ragam penipuan bertambah

Keterampilan pengguna menjadi kunci pemblokir penipu.



## Rekam jejak jadi komoditas

Data bernilai; lebih banyak dimanfaatkan secara negatif.



## Keamanan anak makin menantang

Kecanduan, layanan menarik, dan ruang bermain yang menyempit.

## Solusi: kolaborasi tiga pihak



Individu pengguna



Industri digital



Regulasi yang kuat

*Mengandalkan satu komponen saja tak cukup.*

# Kunci Aman Bermedia Digital



Lindungi perangkat



Jaga identitas & data



Waspada penipuan



Kelola jejak digital



Lindungi anak

*"Saring sebelum sharing. Jarimu harimaumu."*

Keamanan digital adalah tanggung jawab bersama. Terapkan kompetensi analisis, verifikasi, evaluasi, partisipasi, dan kolaborasi untuk melindungi diri sendiri dan sesama warga digital.