TLP : WHITE



# Cyber Security Awareness

## Dark Web : Mengungkap Sisi Tersembunyi Internet & Dampaknya bagi Masyarakat

Suku Dinas Komunikasi, Informatika dan Statistik - Jakarta Barat,

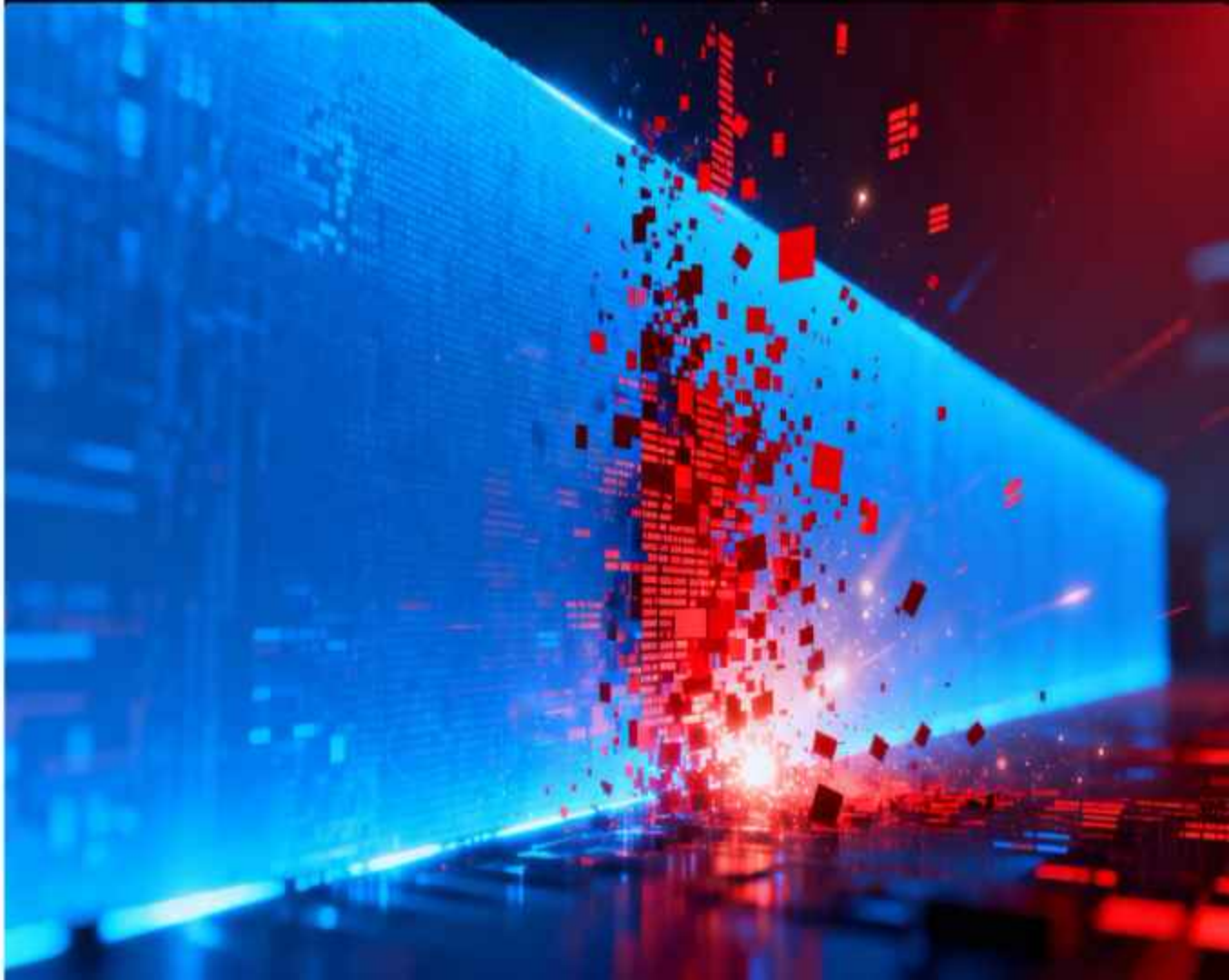
30 April 2026

# Disclaimer

- Materi ini dibuat untuk tujuan edukasi dan kesadaran keamanan siber, bukan untuk mengajarkan atau mendorong aktivitas ilegal.
- Seluruh contoh dan tangkapan layar ditampilkan semata-mata untuk menggambarkan ancaman nyata yang ada di dunia siber.
- Informasi dalam materi ini tidak dimaksudkan sebagai panduan teknis untuk mengakses atau memanfaatkan platform ilegal.
- Penyalahgunaan informasi dalam materi ini sepenuhnya menjadi tanggung jawab individu yang bersangkutan dan dapat dikenakan sanksi hukum sesuai peraturan yang berlaku.

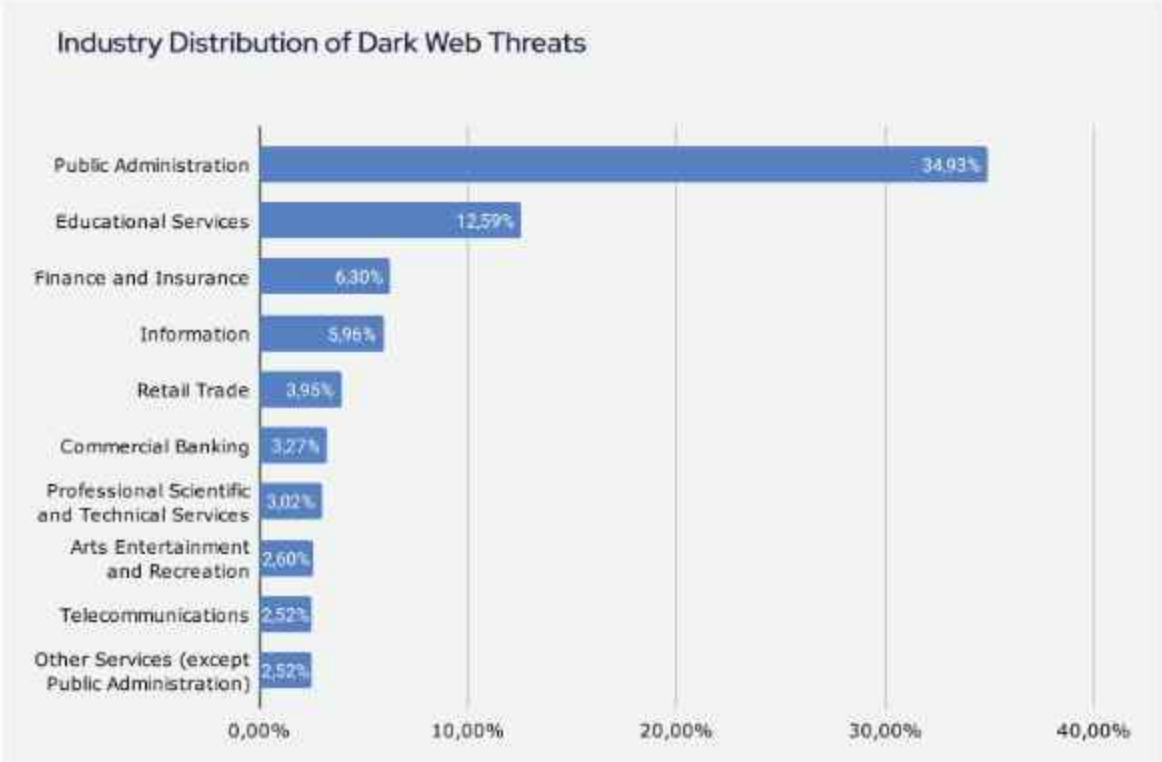
Cyber Security Awareness
Suku Dinas Komunikasi, Informatika dan Statistik

# Indonesia Threat Landscape



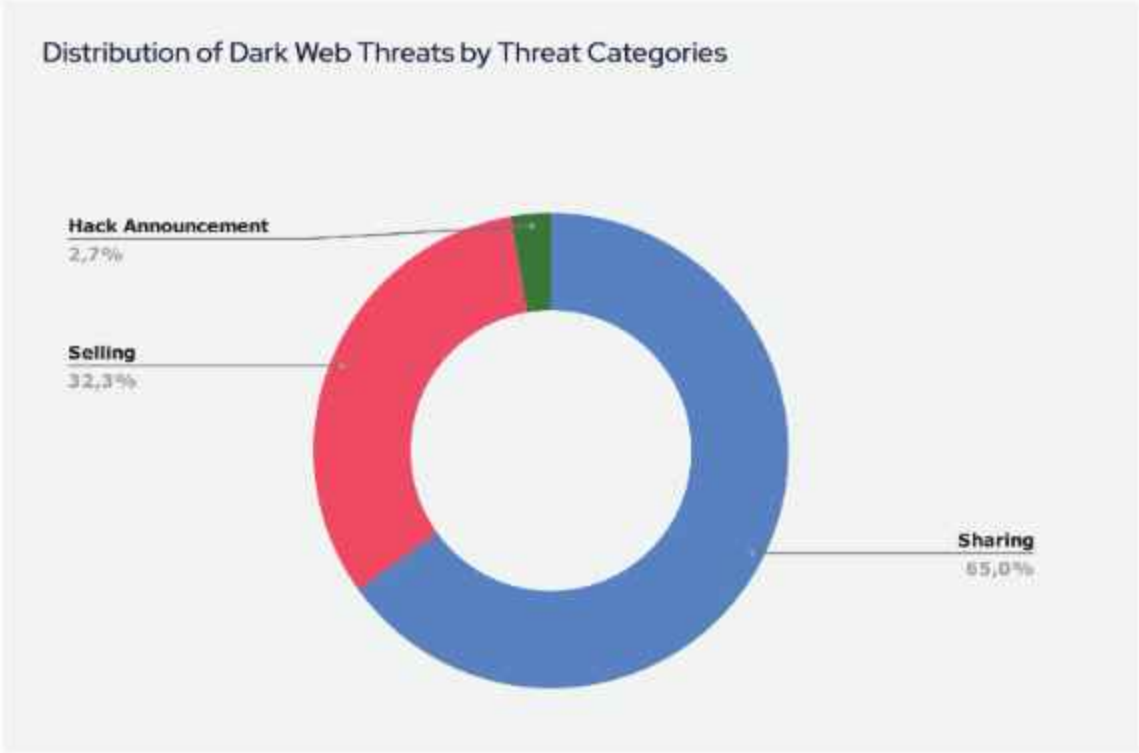
Jakarta Barat - 30 April 2026

# Indonesia Threat Landscape



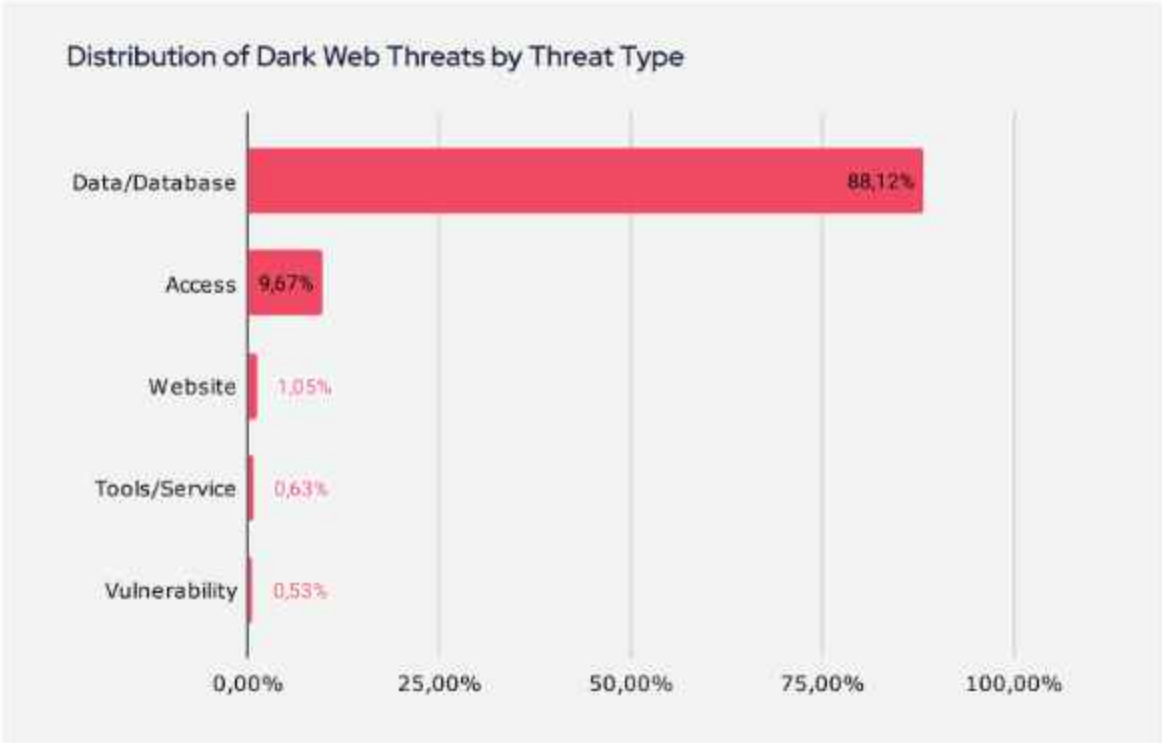

Sumber : Indonesia Regional Threat Landscape Report 2025 - SOC RADAR

# Indonesia Threat Landscape




Sumber : Indonesia Regional Threat Landscape Report 2025 - SOC RADAR

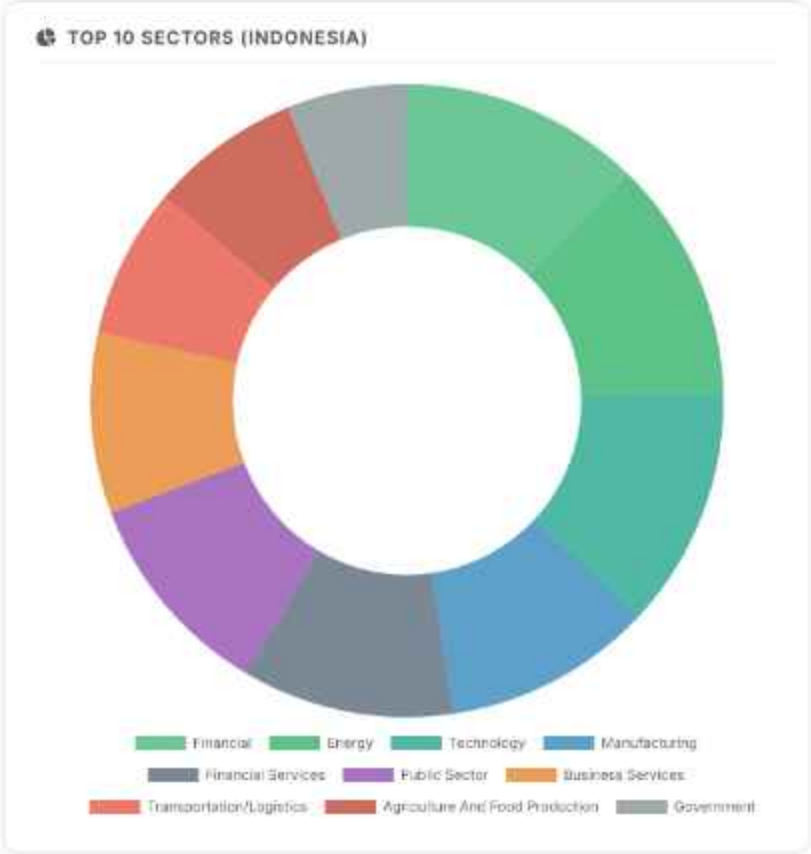
# Indonesia Threat Landscape




Sumber : Indonesia Regional Threat Landscape Report 2025 - SOC RADAR

# Indonesia Threat Landscape

TOTAL VICTIMS
**117**
in Indonesia




Sumber: ransomware.live

# Indonesia Threat Landscape

GROUPS INVOLVED
**48**
in Indonesia


Sumber : ransomware.live

# Indonesia Threat Landscape

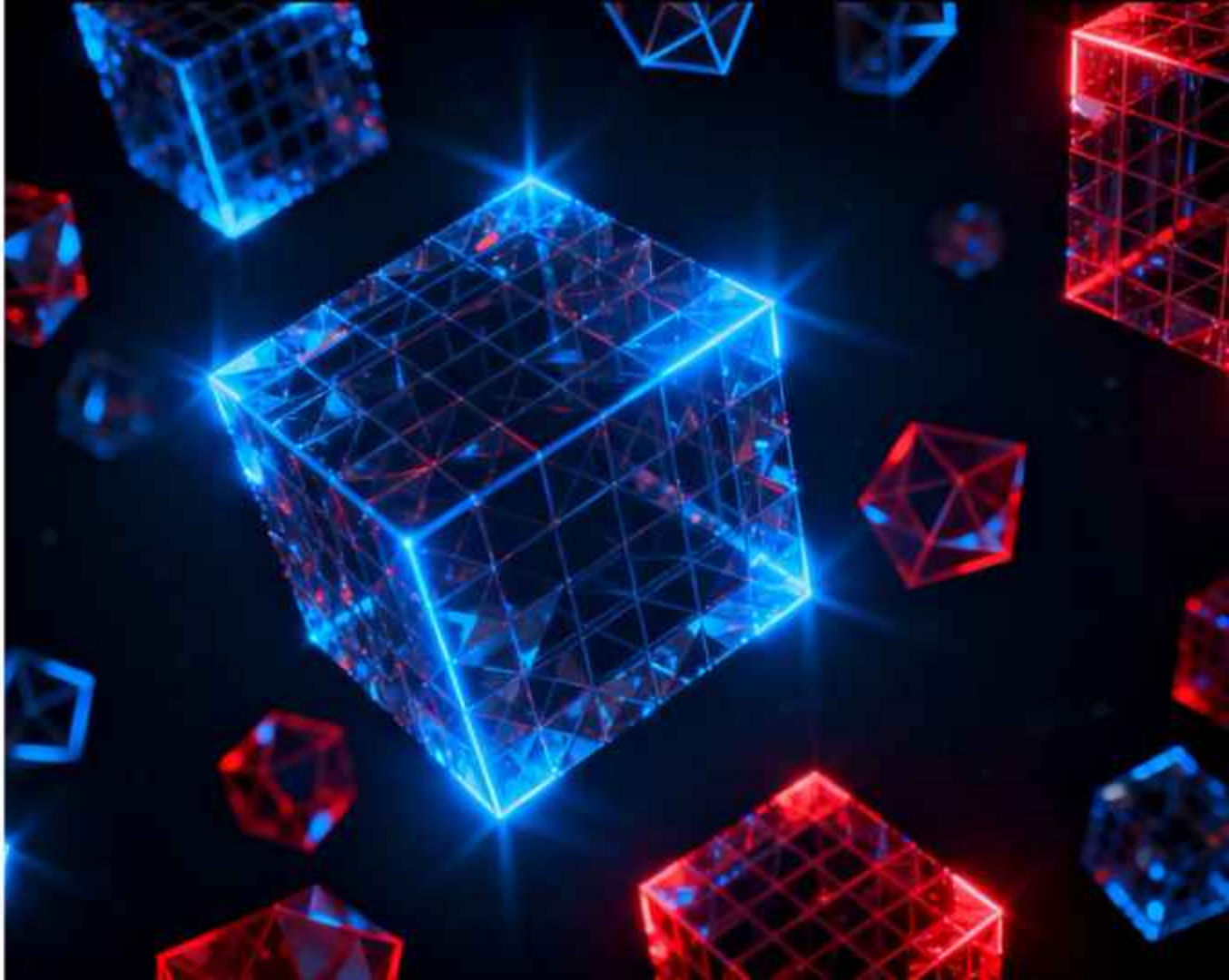
## INFOSTEALERS WEEKLY REPORT

**2026-04-20 - 2026-04-27**


Sumber : Infostealers - Hudson Rock

Cyber Security Awareness
Suku Dinas Komunikasi, Informatika dan Statistik

# Struktur Internet & Area di Dalamnya

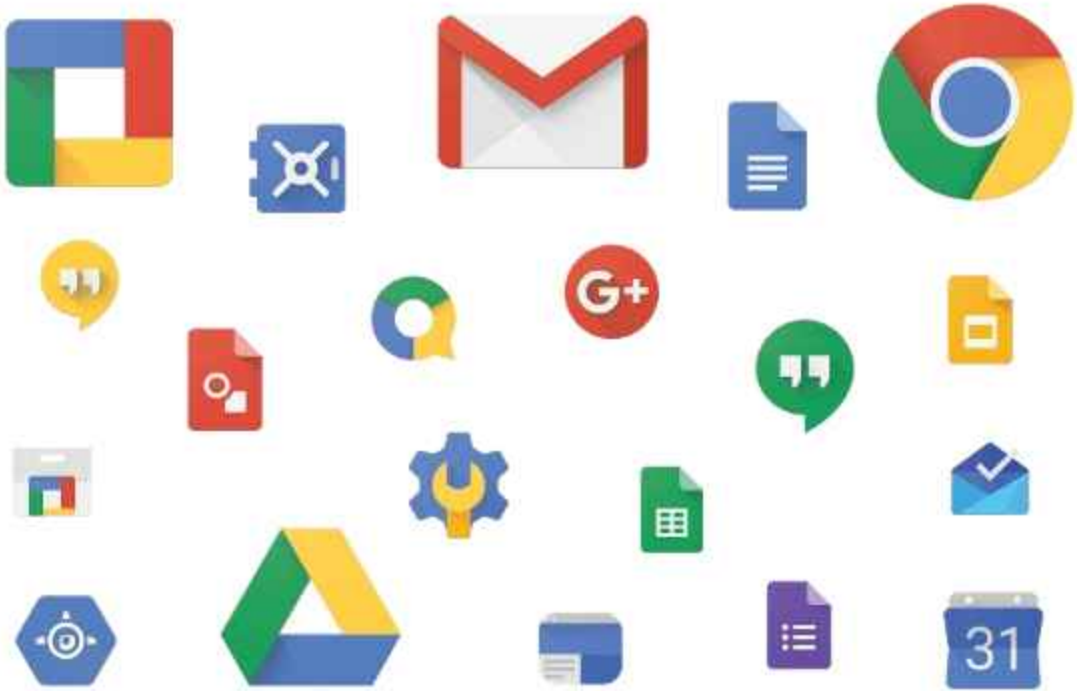


30 April 2026

# Struktur Internet & Area di Dalamnya

Internet ?

# Struktur Internet & Area di Dalamnya



# Struktur Internet & Area di Dalamnya


## Public

- Dapat diakses oleh semua orang
- Bisa ditemukan melalui mesin pencari

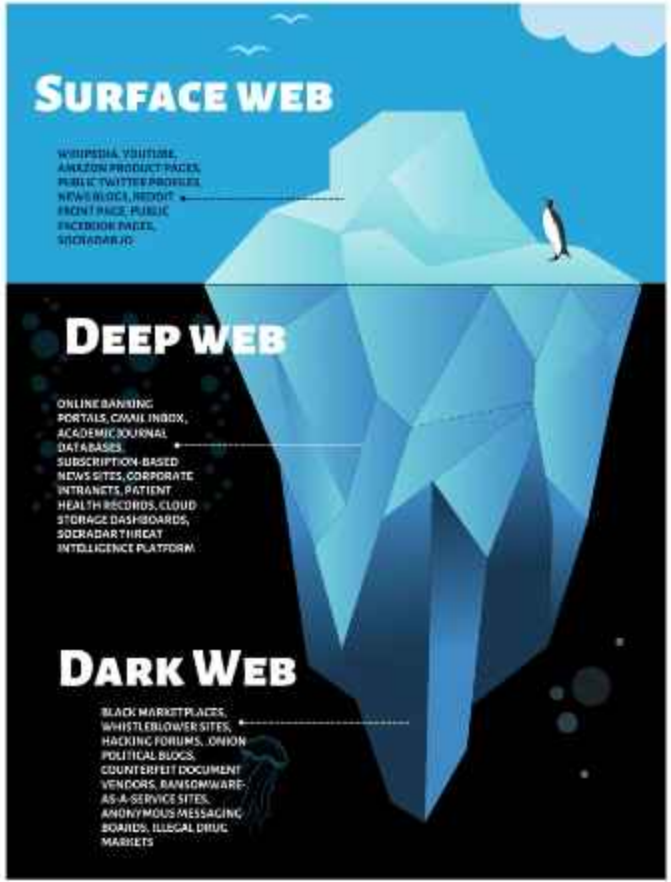
## Private

- Tidak terbuka untuk umum
- Perlu akses khusus

## Hidden

- Tidak terindeks mesin pencari
- Tidak bisa diakses dengan cara biasa
- Menggunakan jaringan/akses khusus

# Struktur Internet & Area di Dalamnya




Sumber : Surface Web Vs Deep Web Vs Dark Web - SOC RADAR

# Struktur Internet & Area di Dalamnya


Bagian internet yang dapat diakses melalui mesin pencari seperti Google atau Bing. Halaman-halaman ini terindeks dan tersedia untuk umum.

Contoh Surface Web :

- Situs berita
- Blog
- Toko online
- Media sosial

Sumber : Surface Web Vs Deep Web Vs Dark Web - SOC RADAR

# Struktur Internet & Area di Dalamnya


Contoh Deep Web :

- Internet banking
- Database perusahaan
- Rekam medis
- Email

Sumber : Surface Web Vs Deep Web Vs Dark Web - SOCRADAR

Bagian internet dengan isi konten yang tidak dapat ditemukan melalui mesin pencari. Dan untuk mengaksesnya, dibutuhkan tautan langsung, akun, atau izin tertentu. Bagian ini legal dan umumnya aman.

# Struktur Internet & Area di Dalamnya


Contoh Dark Web :

- Portal berita independen
- Marketplace ilegal
- Forum aktivitas siber anonim
- Penjualan data hasil peretasan

Sumber : Surface Web Vs Deep Web Vs Dark Web - SOC RADAR

Bagian internet yang merupakan bagian kecil dari Deep Web yang memerlukan cara akses khusus. Bagian ini memungkinkan aktivitas yang lebih anonim serta digunakan untuk layanan tersembunyi dan tidak dapat di akses dengan Browser biasa.

Cyber Security Awareness
Suku Dinas Komunikasi, Informatika dan Statistik

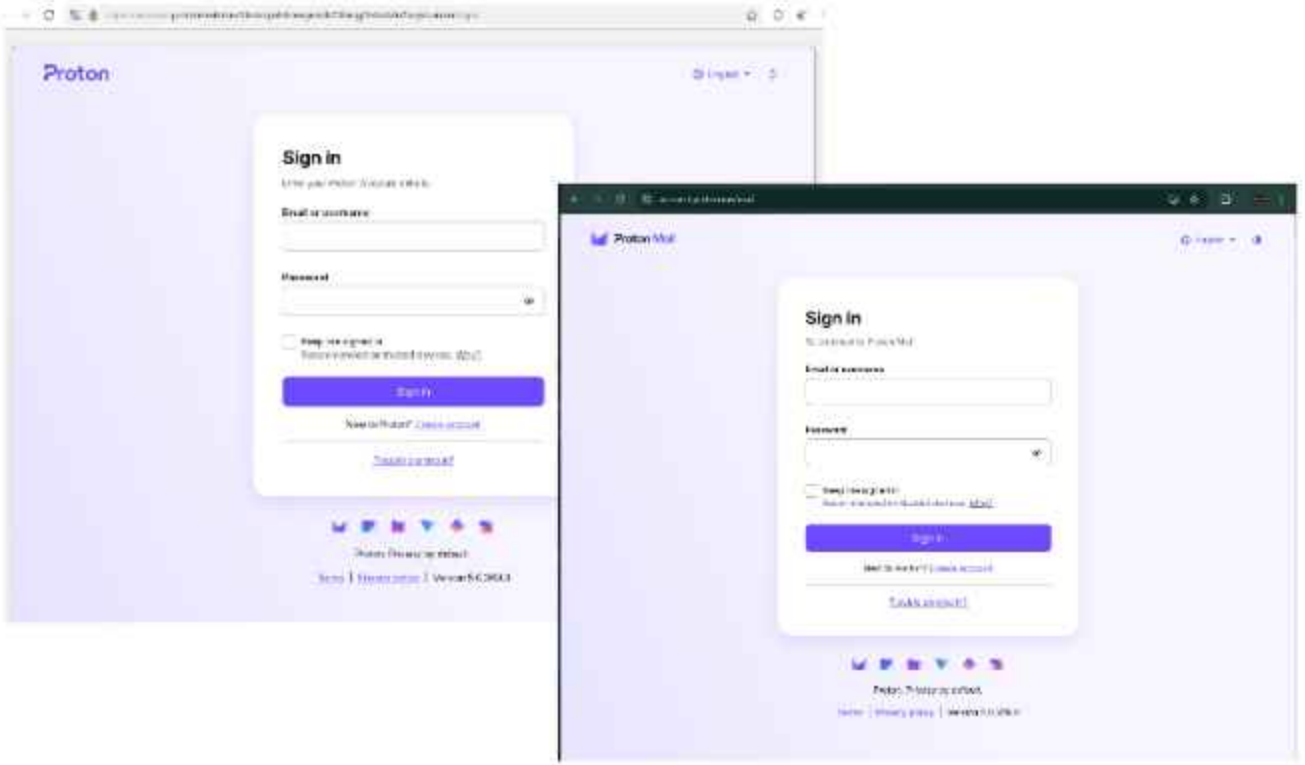
# Dark Web

30 April 2026

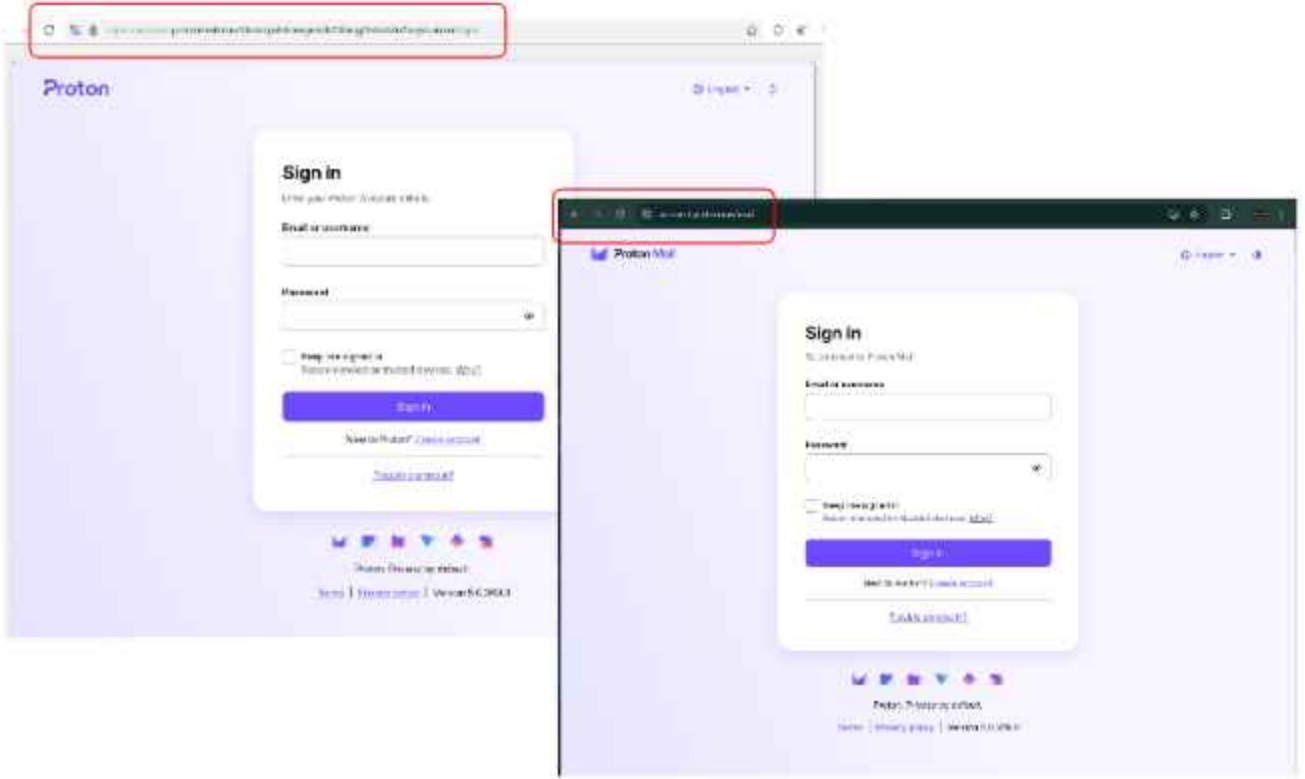
# Dark Web

Bagian internet yang merupakan bagian kecil dari Deep Web yang memerlukan cara akses khusus. Bagian ini memungkinkan aktivitas yang lebih anonim serta digunakan untuk layanan tersembunyi dan tidak dapat di akses dengan Browser biasa.

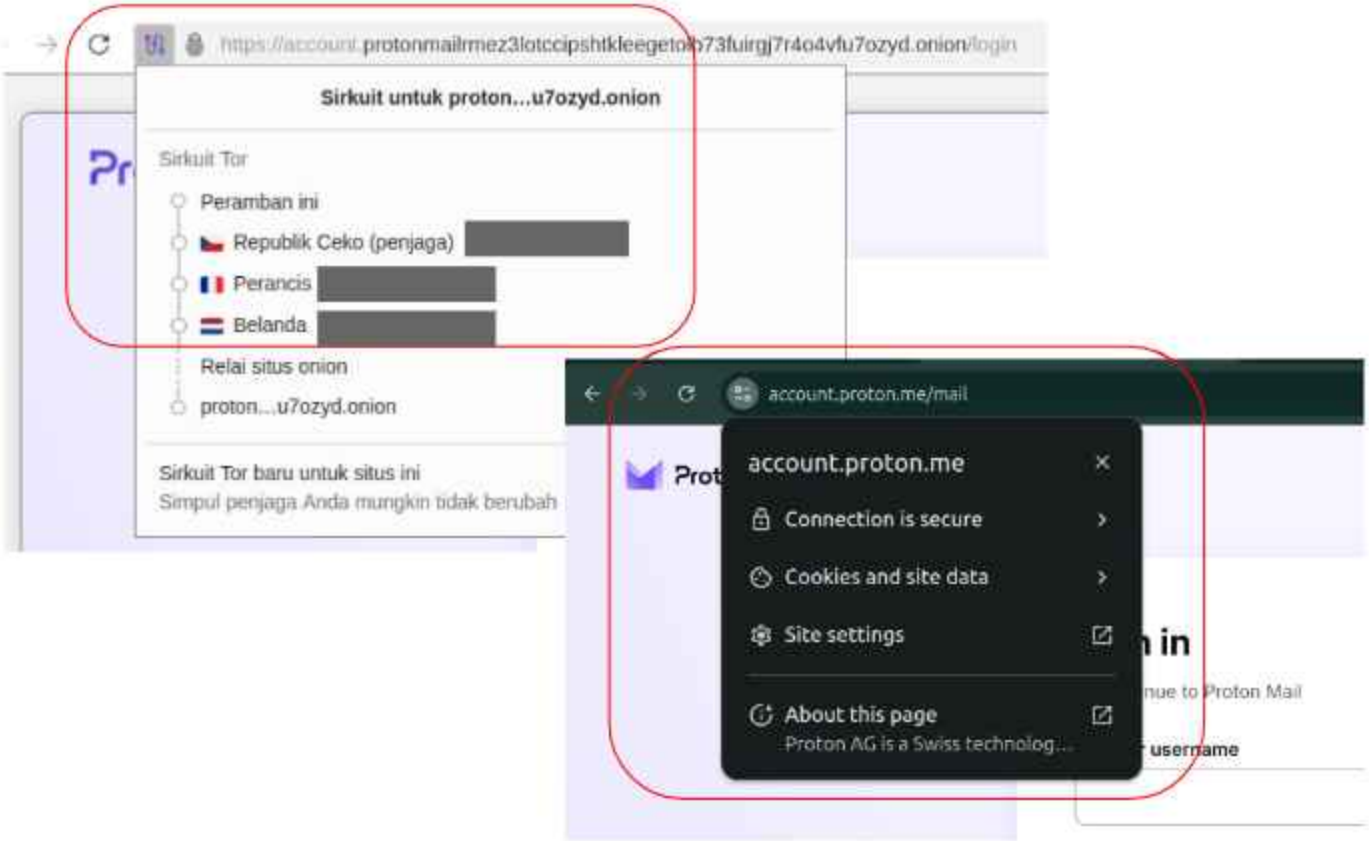
# Dark Web



# Dark Web



# Dark Web



# Dark Web

## Dark Web tidak selalu identik dengan aktivitas ilegal

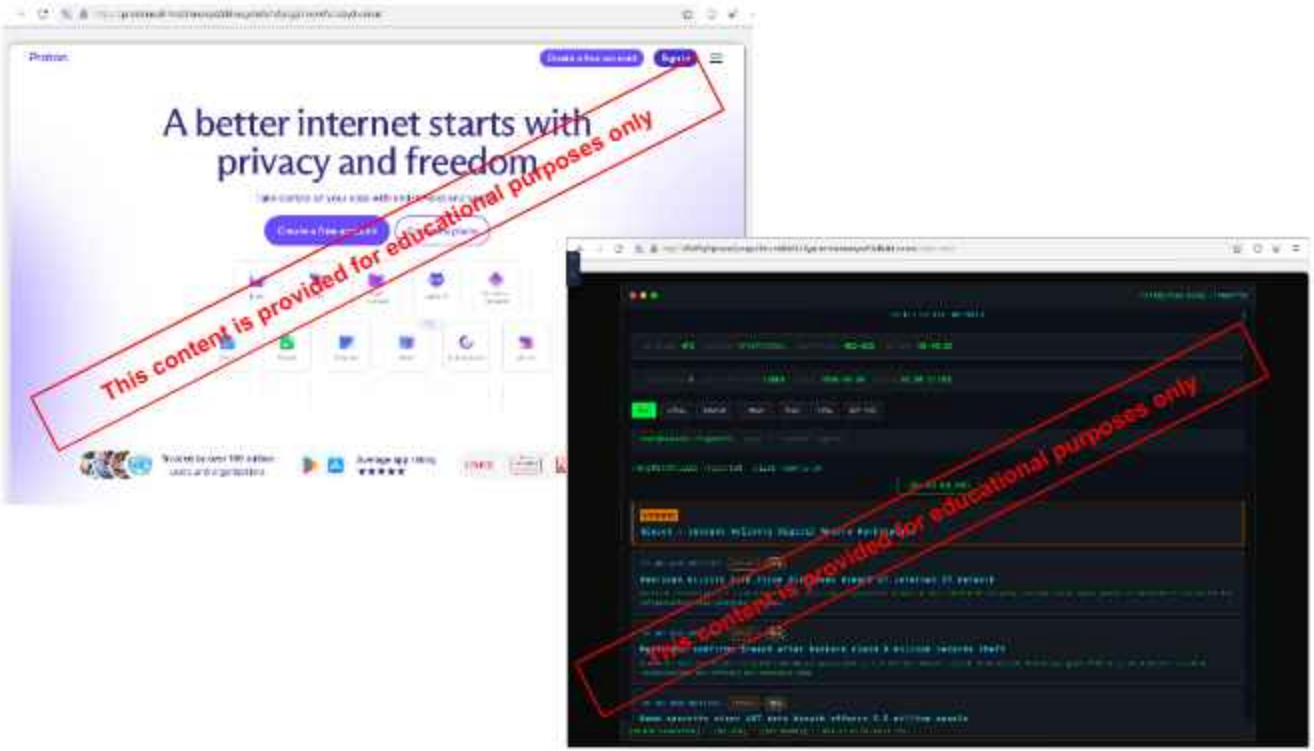
Teknologi ini dirancang untuk memberikan privasi dan anonimitas bagi penggunanya.

Dalam beberapa kondisi, dark web digunakan untuk tujuan yang sah, seperti melindungi identitas pengguna atau mengakses informasi secara aman di lingkungan yang terbatas.

Namun, karena sifatnya yang anonim dan sulit dilacak, dark web juga sering dimanfaatkan untuk aktivitas yang melanggar hukum.

# Dark Web tidak selalu identik dengan aktivitas ilegal

**Dark Web**



# Dark Web

## Penyalahgunaan di Dark Web

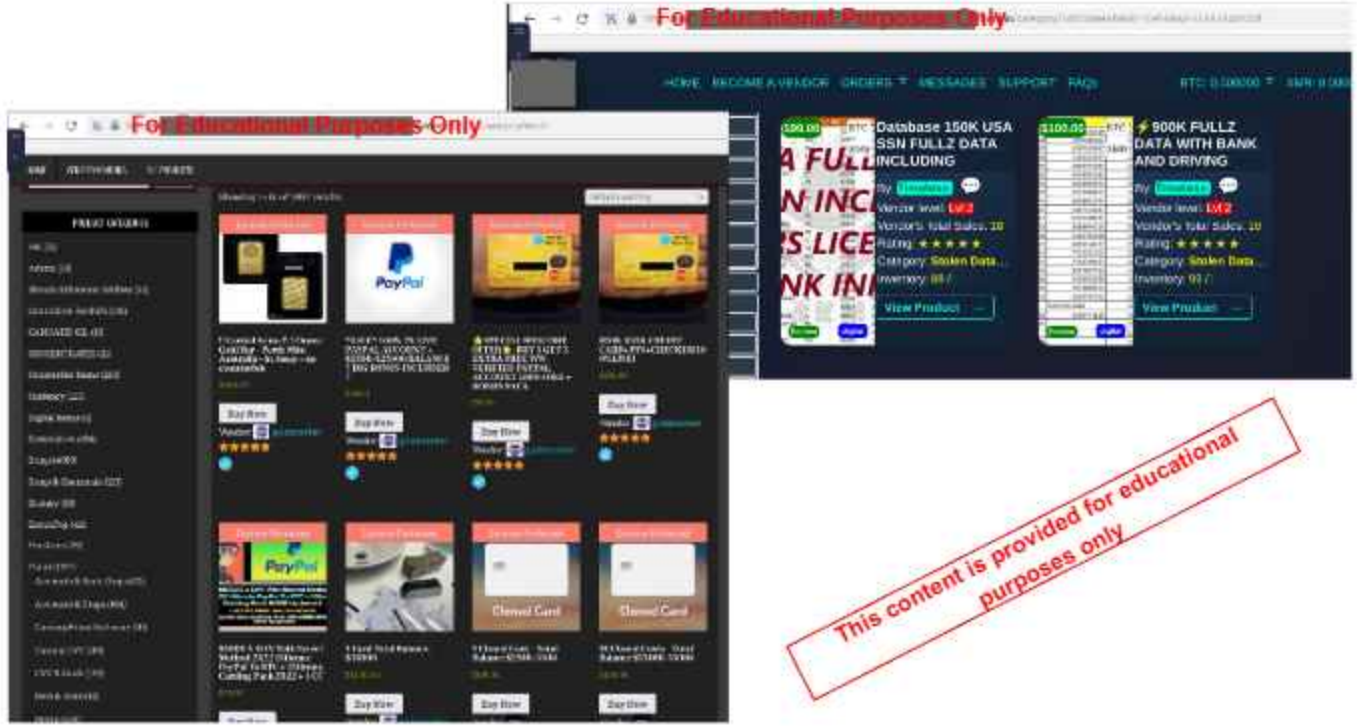
Meskipun memiliki tujuan awal untuk menjaga privasi, dark web sering dimanfaatkan untuk berbagai aktivitas yang merugikan.

Salah satu yang paling umum adalah jual beli data hasil kebocoran, seperti email, password, dan informasi pribadi lainnya.

Selain itu, terdapat juga forum dan komunitas yang membahas aktivitas kejahatan siber, serta berbagai bentuk penipuan yang semakin terorganisir.

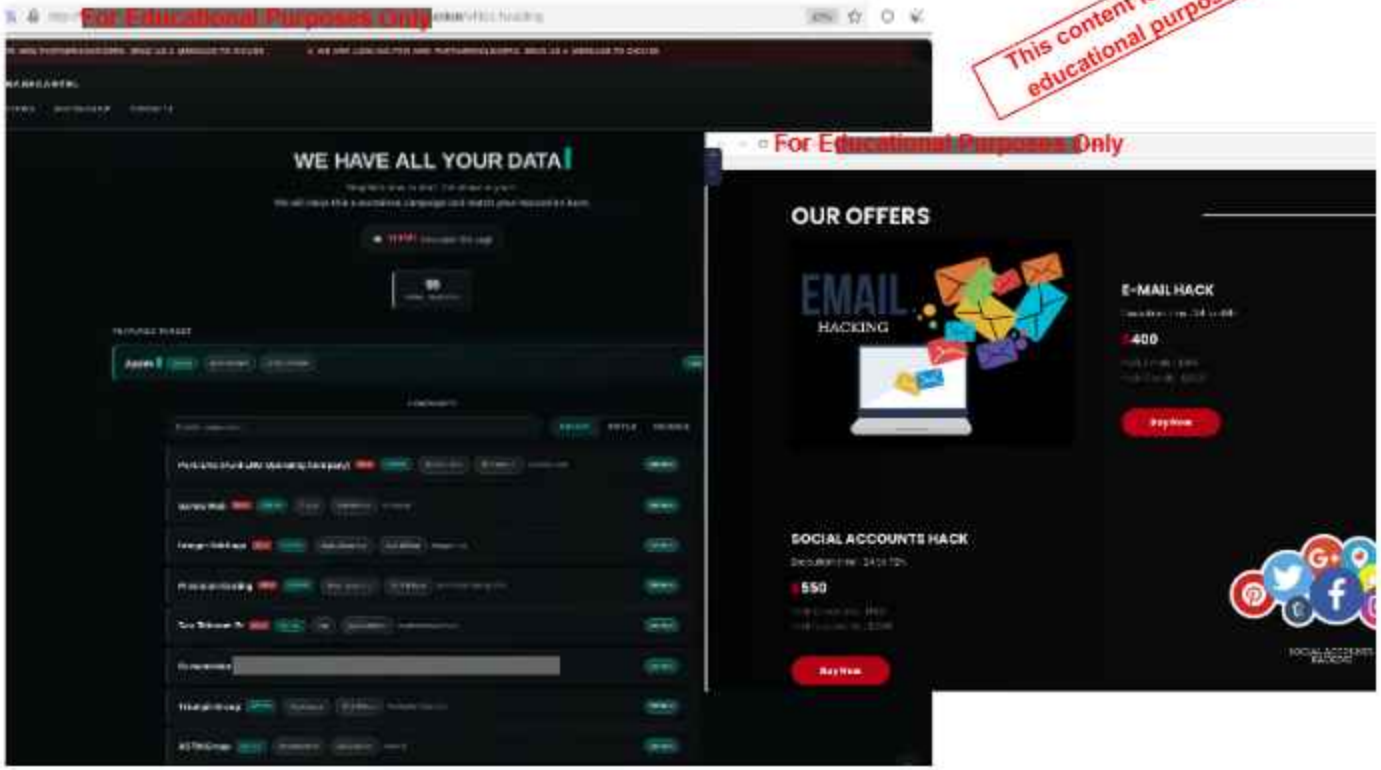
# Penyalahgunaan di Dark Web

Dark Web



# Penyalahgunaan di Dark Web

Dark Web



# Penyalahgunaan di Dark Web

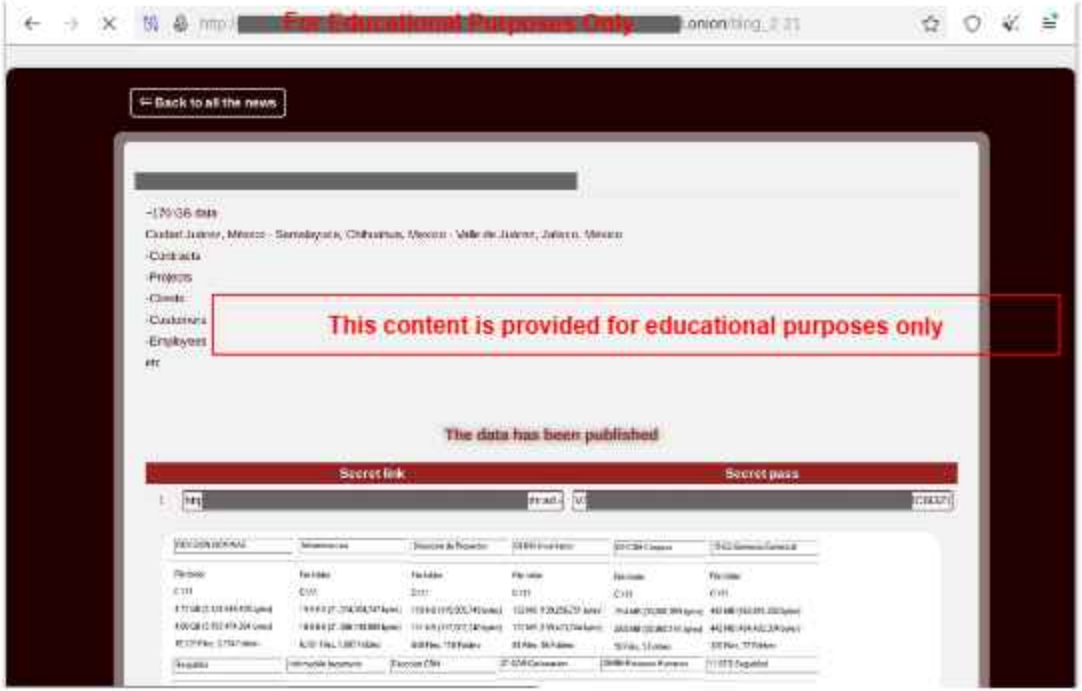
## Dark Web



This content is provided for educational purposes only

# Penyalahgunaan di Dark Web

**Dark Web**



# Penyalahgunaan di Dark Web

Dark Web

Cyber Security Awareness
Suku Dinas Komunikasi, Informatika dan Statistik

# Dampak pada Masyarakat

30 April 2026

# Dampak pada Masyarakat

Aktivitas di dark web **dapat berdampak langsung** pada masyarakat, terutama melalui penyalahgunaan **data pribadi** yang bocor.

Data seperti email, nomor telepon, atau password yang **diperjualbelikan / dibagikan** dapat digunakan untuk berbagai bentuk penipuan, termasuk phishing dan pengambilalihan akun.

Akibatnya, masyarakat dapat mengalami gangguan seperti meningkatnya **spam**, percobaan **penipuan** yang lebih meyakinkan, hingga kerugian finansial.

# Dampak pada Masyarakat

Selasa, 28 April 2026

RADAR BOJONEGORO

Daerah | Ekonomi | Gemas | Haji & Umrah | Headline News | Internasional | Kawan Cilik | Lainnya

**10.583 Kasus Penipuan Online Awal 2026: Aneka Investasi Bodong dan Jaringan Scam Kamboja Terbongkar!**

Bhagas Dani Purwoko
Selasa, 28 Apr 2026 | 15:55 WIB

Share

Warta Kepri

**OJK Kepri Waspadai Lonjakan Kejahatan Siber, Ribuan Kasus Penipuan Terungkap**

TEMPO

Menu | Harian | Mingguan | Tempo Plus

Digital

**Benarkah Data 240 Juta Penduduk Indonesia Dijual di Dark Web**

Beredar di media sosial tangkapan layar yang menampilkan klaim kebocoran "240 Million Population Database" Indonesia. Respons pakar mengejutkan.

# Dampak pada Masyarakat

TEMPO

Menu Harian Mingguan Tempo Plus

Ekonomi Ekonomi Sinyal Pasar Bisnis Kelestarian

**15 Juta Data Nasabah BSI Diduga Bocor, Pakar Siber: Hati-hati Serangan Phising ke Pemilik Rekening**

Data nasabah Bank Syariah Indonesia atau BSI diduga bocor. Pakar keamanan siber peringatkan potensi serangan phising dan scamming.

16 Mei 2023 | 19.55 WIB

kompasiana

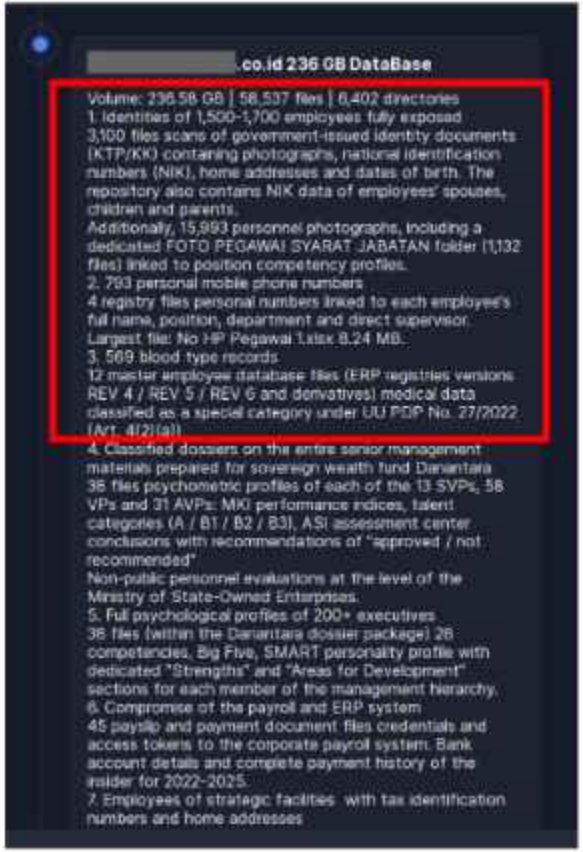
Program Terpopuler Terbaru Headline Topik Pilihan

Ramadan Sustainability Lyfe Money Vox Pop Travel Story Halo Lokal

**Kebocoran Data BPJS Ketenagakerjaan Diduga Terulang Kembali, Data Masyarakat Indonesia Terancam**

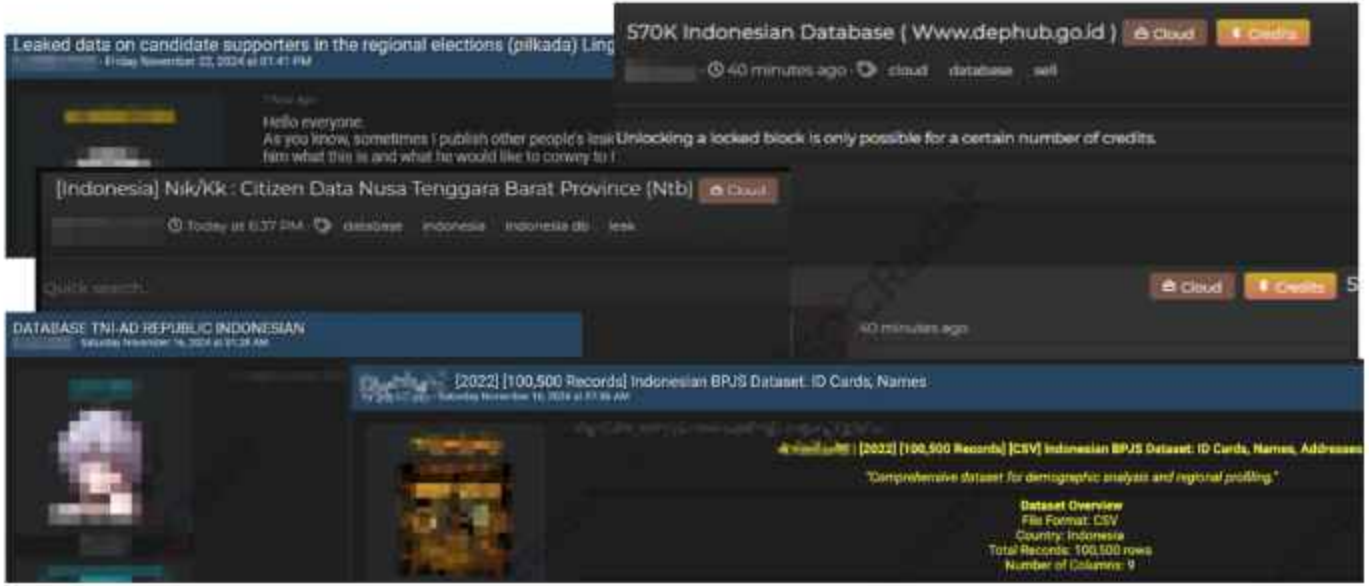
# Dampak pada Masyarakat

# Dampak pada Masyarakat




- Data pribadi di KTP/KK
- Nomor Telpon
- Data pekerjaan dan jabatan
- Golongan darah
- Profil psikologi
- Data payroll

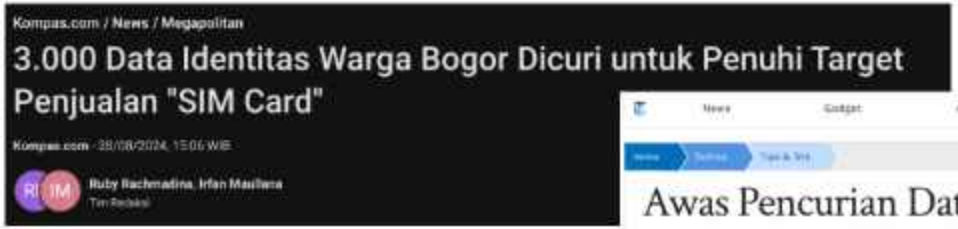
# Dampak pada Masyarakat



# Dampak pada Masyarakat

# Dampak pada Masyarakat


# Dampak pada Masyarakat


Kompas.com / News / Megapolitan

3.000 Data Identitas Warga Bogor Dicuri untuk Penuhi Target Penjualan "SIM Card"

Kompas.com - 28/08/2024, 15:06 WIB

Ruby Rachmadina, Irfan Maullana

Tim Redaksi


Awas Pencurian Data Pribadi lewat Smartphone, Kenali Ciri-Ciri Malware APK!


CNBC Indonesia > Tech > Berita Tech

1,4 Juta Data Kesehatan Bocor, Terbesar Sepanjang 2024

Redaksi, CNBC Indonesia

05 August 2024 21:20

# Dampak pada Masyarakat

Data yang bocor bukan hanya disalahgunakan secara teknis, tapi juga dimanfaatkan untuk meyakinkan korban secara psikologis melalui **Social Engineering**.

Dengan berbekal nama, nomor telepon, dan alamat korban yang didapat dari dark web, pelaku mampu menyusun skenario penipuan yang **terasa sangat meyakinkan**.

# Dampak pada Masyarakat

KOMPAS.com News Kolom Event Cahaya Tekno Otomotif Bola Lifestyle Tren Lestari Money Properti Edukasi Trav

BAGIKAN: Komdigi: 60 Persen Pengguna Seluler Terima "Spam Call" Minimal Satu Minggu Se... KOMENTAR:

Kompas.com / News / Nasional

## Komdigi: 60 Persen Pengguna Seluler Terima "Spam Call" Minimal Satu Minggu Sekali

Kompas.com, 27 Januari 2026, 20:16 WIB

Add on Google

Firda Janati, Robertus Belarminus

Tim Redaksi

# Dampak pada Masyarakat



Cyber Security Awareness
Suku Dinas Komunikasi, Informatika dan Statistik

# Aspek Hukum


30 April 2026

# Aspek Hukum

Aktivitas di dunia digital, termasuk yang berkaitan dengan penyalahgunaan data dan kejahatan siber, telah diatur dalam berbagai **peraturan perundang-undangan** di Indonesia.

Regulasi ini bertujuan untuk **melindungi masyarakat** dari penyalahgunaan data pribadi serta memberikan sanksi bagi pelaku kejahatan siber.

# Aspek Hukum

Beberapa regulasi yang mengatur keamanan digital dan perlindungan data di Indonesia antara lain:

- Undang-Undang Informasi dan Transaksi Elektronik (UU ITE)
- Undang-Undang Perlindungan Data Pribadi (UU PDP)
- Peraturan terkait keamanan sistem elektronik

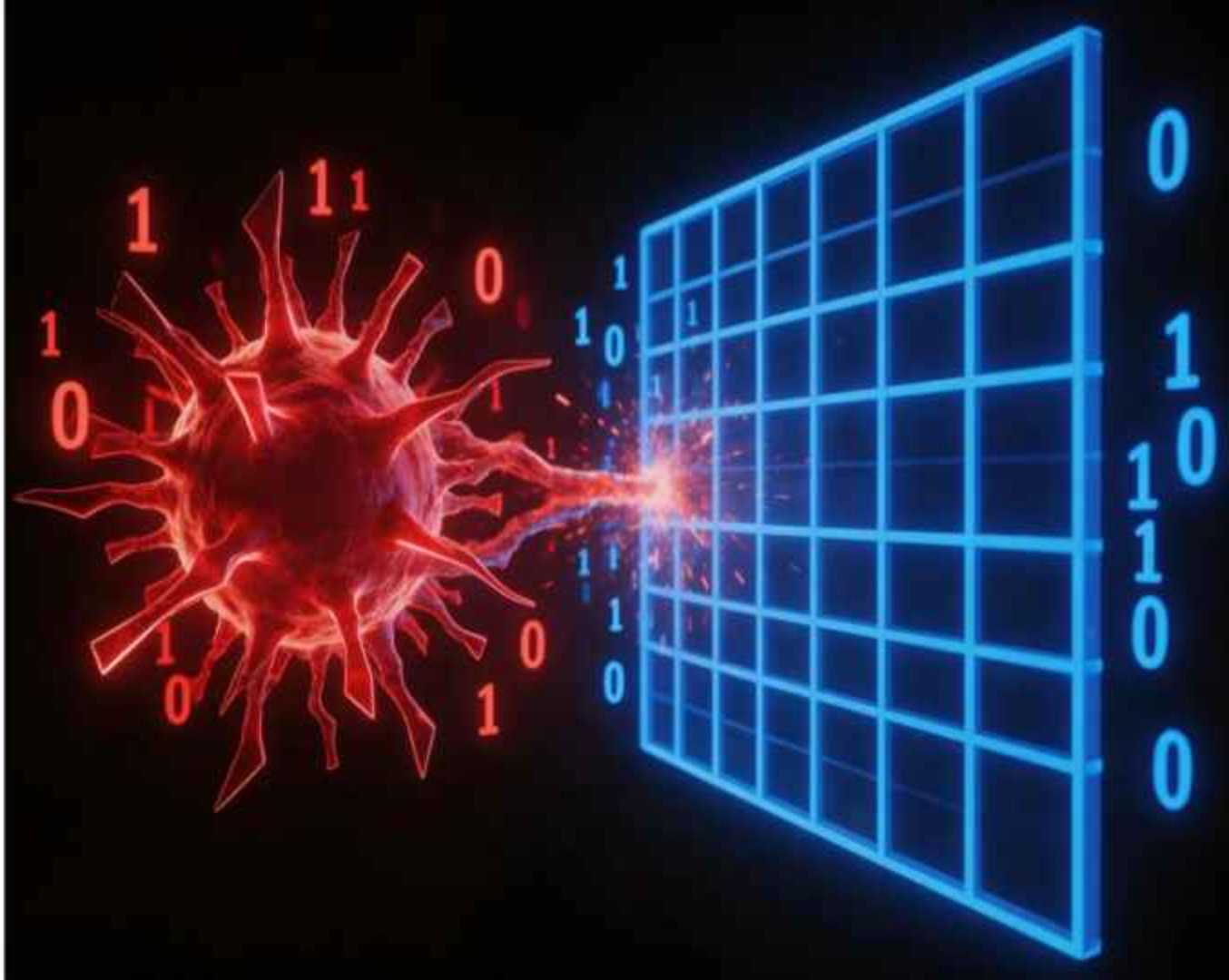
# Aspek Hukum

**Ketidaktahuan** terhadap regulasi **tidak menghapus tanggung jawab** hukum.

**Mengetahui** aturan adalah **bagian dari kontribusi** kita menjaga keamanan digital bersama.

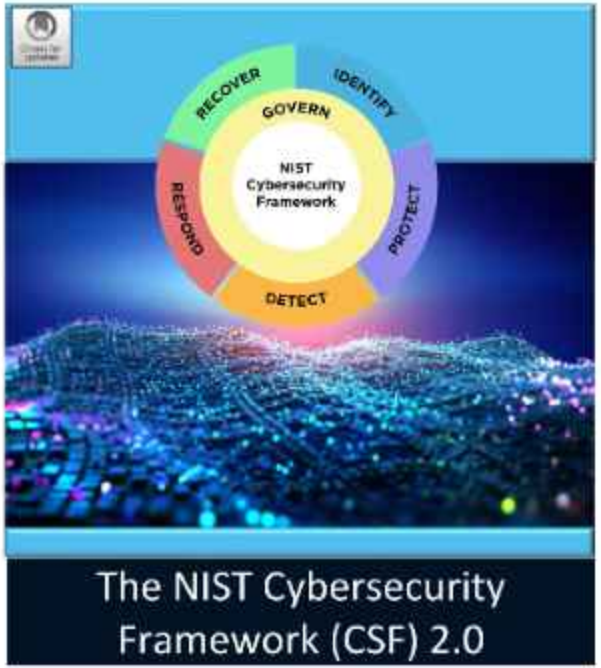
Cyber Security Awareness
Suku Dinas Komunikasi, Informatika dan Statistik

# Standar Keamanan



30 April 2026

# Standar Keamanan




Framework keamanan siber yang dikembangkan oleh National Institute of Standards and Technology (AS) untuk membantu organisasi mengelola dan mengurangi risiko siber. Terdiri dari 6 fungsi inti:

- Govern
- Identify
- Protect
- Detect
- Respond
- Recover

# Standar Keamanan

SNI
Standar Nasional Indonesia

SNI ISO/IEC 27001:2022
(Ditetapkan oleh BSN tahun 2023)

**Keamanan informasi, keamanan siber, dan proteksi privasi — Sistem manajemen keamanan informasi — Persyaratan**

**Information security, cybersecurity and privacy protection — Information security management systems — Requirements**

(ISO/IEC 27001:2022, IDT)

ICS 35.030, 03.100.70

BSN BADAN STANDARDISASI NASIONAL

Standar internasional untuk Sistem Manajemen Keamanan Informasi. Memberikan kerangka kerja dalam menetapkan, menerapkan, memelihara, dan terus meningkatkan keamanan informasi secara sistematis. Kontrol keamanan dikelompokkan dalam 4 tema:

- Organisational
- People
- Physical
- Technological

# Standar Keamanan

PERATURAN BANK INDONESIA
NOMOR 2 TAHUN 2024
TENTANG
KEAMANAN SISTEM INFORMASI DAN KETAHANAN SIBER BAGI PENYELENGGARA SISTEM PEMBAYARAN, PELAKU PASAR UANG DAN PASAR VALUTA ASING, SERTA PIHAK LAIN YANG DIATUR DAN DIAWASI BANK INDONESIA

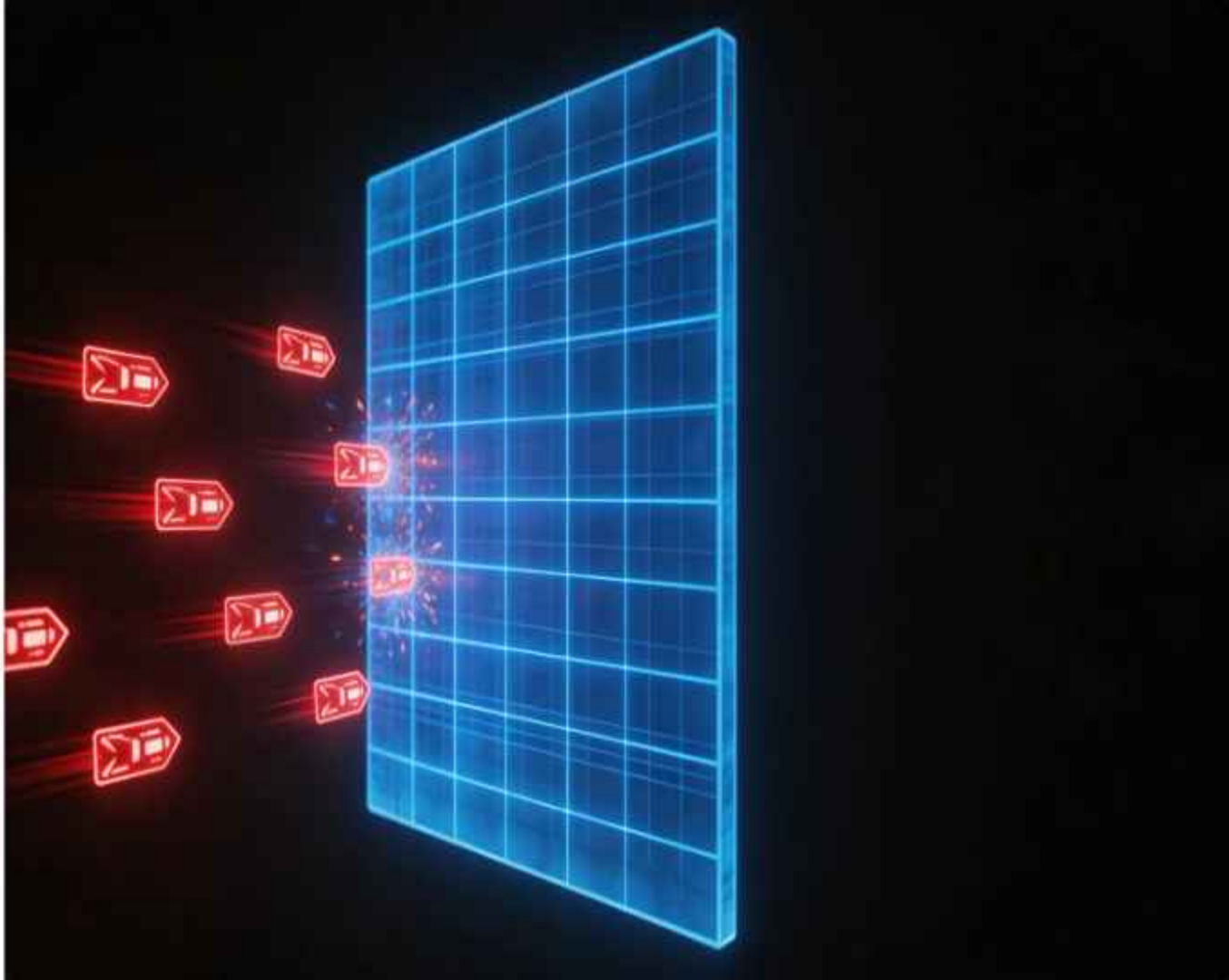
DENGAN RAHMAT TUHAN YANG MAHA ESA


Regulasi Bank Indonesia yang mengatur penerapan keamanan sistem informasi dan ketahanan siber bagi penyelenggara sistem pembayaran, pelaku pasar uang dan pasar valuta asing, serta pihak lain yang diawasi Bank Indonesia. Ruang lingkup pengaturan mencakup :

- Strategi dan Kebijakan
- Budaya
- Identifikasi
- Proteksi
- Deteksi
- Respond
- Pemulihan

Cyber Security Awareness
Suku Dinas Komunikasi, Informatika dan Statistik

# Langkah Perlindungan



30 April 2026

# Langkah Perlindungan

- Sebelum Terjadi
- Setelah Terjadi

# Langkah Perlindungan

## Sebelum Terjadi

- Kenali dan catat aset digital yang dimiliki, seperti akun aktif, perangkat yang digunakan, dan data pribadi yang tersimpan secara online. Dengan mengetahui apa yang perlu dilindungi, kita dapat lebih fokus dalam menjaga keamanannya.
  Referensi : ISO 27001:2022 — A.5.9 Inventori informasi dan aset terkait lainnya | NIST CSF 2.0 — ID.AM-08

- Gunakan password yang kuat, panjang, dan unik untuk setiap akun yang dimiliki. Hindari menggunakan password yang sama di lebih dari satu layanan, karena satu akun yang bocor bisa berdampak ke akun lainnya.
  Referensi : ISO 27001:2022 — A.5.17 Informasi autentikasi | NIST CSF 2.0 — PR.AA-01

- Aktifkan autentikasi dua faktor (2FA) di semua akun penting seperti email, media sosial, dan perbankan. Lapisan keamanan tambahan ini memastikan bahwa meskipun password bocor, akun tetap tidak bisa diakses sembarangan.
  Referensi : ISO 27001:2022 — A.5.17 Informasi autentikasi & A.8.5 Autentikasi aman | NIST CSF 2.0 — PR.AA-01

# Langkah Perlindungan

## Sebelum Terjadi

- Pastikan software, aplikasi, dan sistem operasi yang digunakan selalu dalam versi terbaru. Pembaruan rutin menutup celah keamanan yang berpotensi dieksploitasi oleh pelaku kejahatan siber.
  Referensi : ISO 27001:2022 — A.8.8 Manajemen kerentanan teknis | NIST CSF 2.0 — PR.PS-02

- Hanya unduh aplikasi dari sumber resmi seperti Play Store atau App Store, dan hindari menginstal file APK dari sumber tidak dikenal. Aplikasi tidak resmi sering kali menjadi media penyebaran malware dan infostealer.
  Referensi : ISO 27001:2022 — A.8.19 Instalasi perangkat lunak pada sistem operasional | NIST CSF 2.0 — PR.PS-02 & PR.PS-05

- Batasi informasi pribadi yang dibagikan di platform publik, termasuk nomor telepon, alamat, dan tanggal lahir. Data yang terlihat sepele sekalipun bisa dimanfaatkan untuk menyusun profil korban di dark web.
  Referensi : ISO 27001:2022 — A.5.12 Klasifikasi informasi & A.5.34 Privasi dan proteksi PII | NIST CSF 2.0 — ID.AM-05 & PR.DS

# Langkah Perlindungan

## Setelah Terjadi

- Segera **ganti password** akun yang terdampak atau diduga ikut bocor dalam suatu insiden. Jangan tunda, karena semakin cepat diganti semakin kecil peluang akun disalahgunakan.

  Referensi : ISO 27001:2022 – A.5.26 Respons terhadap insiden keamanan informasi | NIST CSF 2.0 – RS.MI-01

- **Aktifkan 2FA** apabila sebelumnya belum diaktifkan, terutama di akun yang berkaitan dengan data sensitif atau finansial. Ini menjadi lapisan pertahanan tambahan meskipun password sudah terlanjur diketahui pihak lain.

  Referensi : ISO 27001:2022 – A.8.5 Autentikasi aman | NIST CSF 2.0 – RS.MA-01 & PR.AA-01

# Langkah Perlindungan

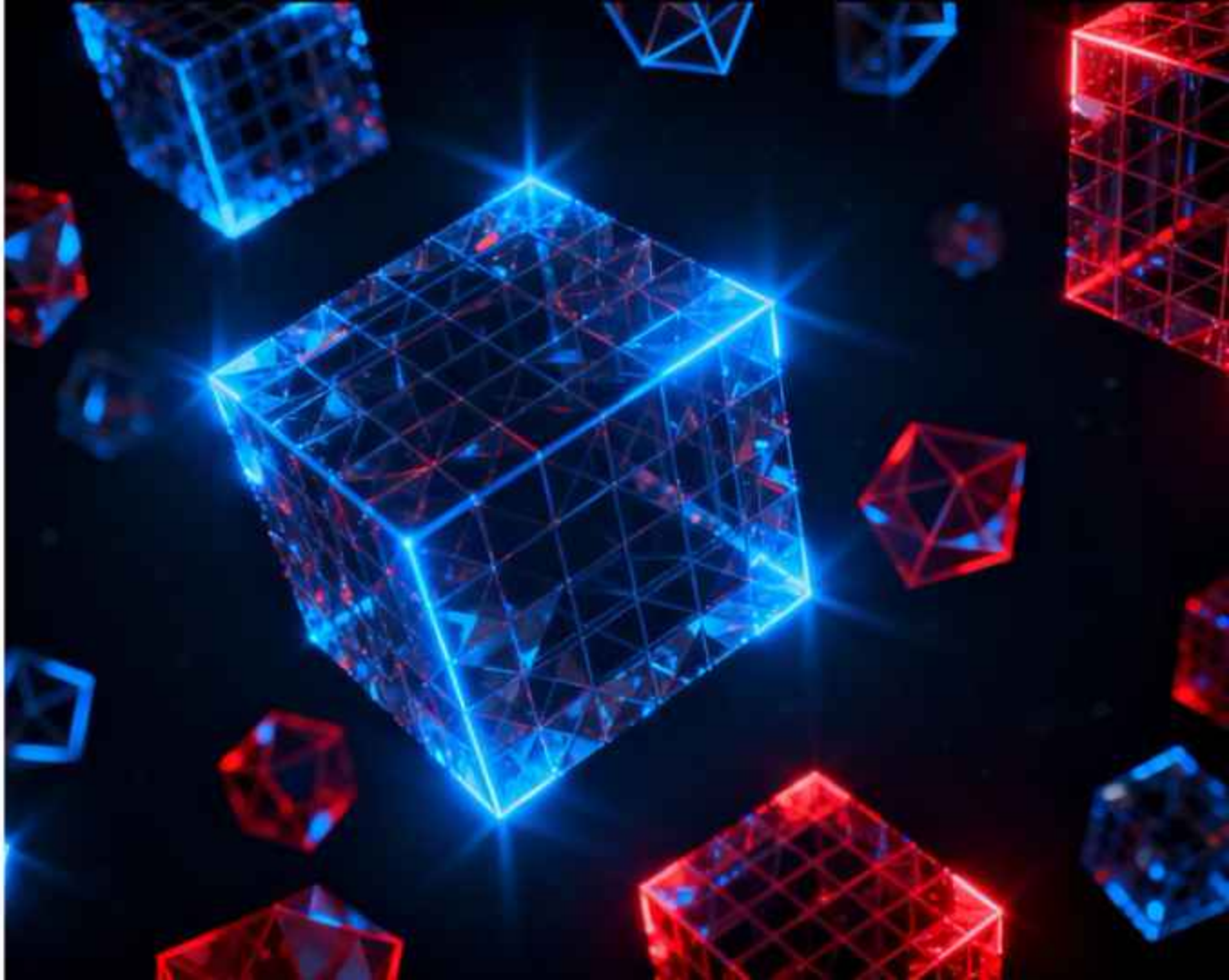
## Setelah Terjadi

- **Pantau aktivitas mencurigakan** di akun dan perangkatmu secara berkala setelah insiden terjadi. Pelaku yang telah mendapatkan akses awal sering kali mencoba masuk kembali dalam jangka waktu tertentu.
  Referensi : ISO 27001:2022 – A.8.16 Pemonitoran aktivitas | NIST CSF 2.0 – DE.CM-03

- **Hapus data pribadi** yang sudah tidak diperlukan dari perangkat maupun layanan yang digunakan. Meminimalkan jejak data yang tersimpan akan mengurangi risiko kerugian apabila insiden serupa terjadi di masa mendatang.
  Referensi : ISO 27001:2022 – A.8.10 Penghapusan informasi | NIST CSF 2.0 – PR.DS-01

Cyber Security Awareness
Suku Dinas Komunikasi, Informatika dan Statistik

# Kontribusi Bersama



30 April 2026

# Kontribusi Bersama

**Keamanan siber** bukan hanya tanggung jawab organisasi atau penyedia layanan, tetapi juga menjadi **tanggung jawab bersama** sebagai pengguna internet.

**Setiap individu memiliki peran penting** dalam menjaga keamanan data pribadi dan mencegah penyalahgunaan informasi di dunia digital.

Melalui **kebiasaan** yang tepat dan **kesadaran** yang baik, risiko terhadap kejahatan siber dapat diminimalkan.

# Kontribusi Bersama

## DO


## DON'T

# Kontribusi Bersama

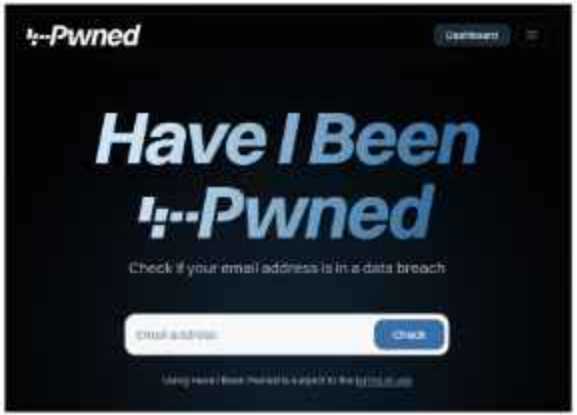
## DO

Proton Pass
NordPass
RememBear
1Password
Zoho Vault
LogMeOnce

## DON'T

# Kontribusi Bersama

## DO



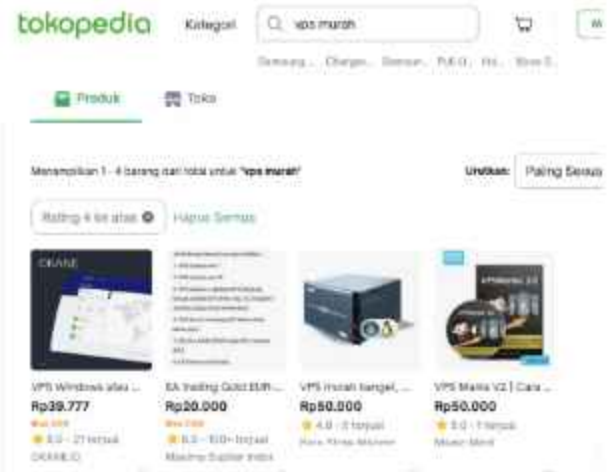

## DON'T


Referensi : ISO 27001:2022 — A.5.17 Informasi autentikasi | NIST CSF 2.0 — PR.AA-01

# Kontribusi Bersama

## DO


## DON'T



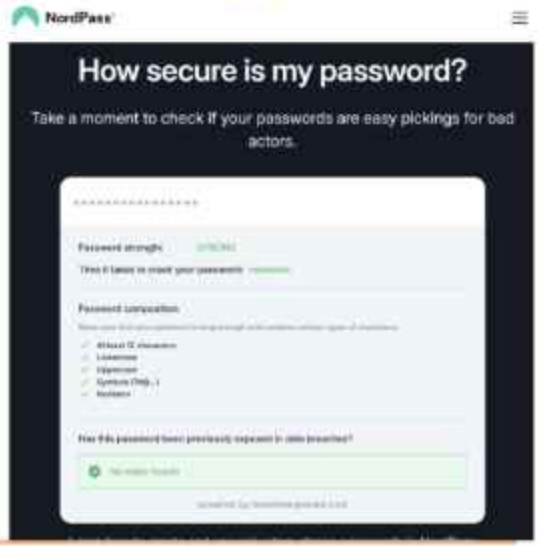
# Kontribusi Bersama

## DO


## DON'T

# Kontribusi Bersama

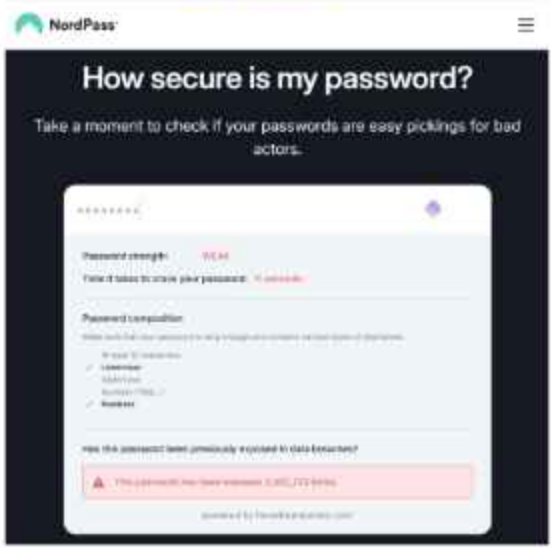
## DO




NordPass
https://nordpass.com › secu... · Terjemahkan

How Secure Is My Password?

## DON'T




Referensi : ISO 27001:2022 — A.5.17 Informasi autentikasi | NIST CSF 2.0 — PR.AA-01

# Kontribusi Bersama

## DO


## DON'T

Referensi : ISO 27001:2022 — A.8.7 Proteksi terhadap perangkat perusak | NIST CSF 2.0 — PR.IR-02

# Kontribusi Bersama

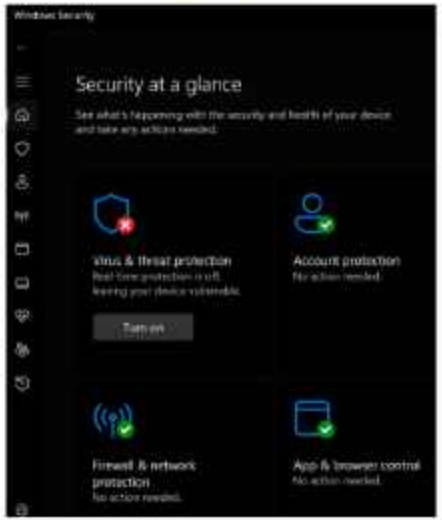
## DO


## DON'T

# Kontribusi Bersama

## DO


## DON'T




Referensi : ISO 27001:2022 — A.8.7 Proteksi terhadap perangkat perusak | NIST CSF 2.0 — PR.IR-02

# Kontribusi Bersama

## DO


## DON'T


Referensi : ISO 27001:2022 — A.8.5 Autentikasi aman | NIST CSF 2.0 — PR.AA-01

# Kontribusi Bersama

## DO


## DON'T


Referensi : ISO 27001:2022 — A.5.17 Informasi autentikasi & A.8.5 Autentikasi aman | NIST CSF 2.0 — PR.AA-01

# Kontribusi Bersama

## DO


## DON'T

# Disclaimer

- Materi ini dibuat untuk tujuan edukasi dan kesadaran keamanan siber, bukan untuk mengajarkan atau mendorong aktivitas ilegal.
- Seluruh contoh dan tangkapan layar ditampilkan semata-mata untuk menggambarkan ancaman nyata yang ada di dunia siber.
- Informasi dalam materi ini tidak dimaksudkan sebagai panduan teknis untuk mengakses atau memanfaatkan platform ilegal.
- Penyalahgunaan informasi dalam materi ini sepenuhnya menjadi tanggung jawab individu yang bersangkutan dan dapat dikenakan sanksi hukum sesuai peraturan yang berlaku.

# Feel free to reach out

taufik.hdyth@protonmail.com

/in/taufik-hidytllah

TLP : WHITE

# Terimakasih

Dark Web : Mengungkap Sisi Tersembunyi Internet & Dampaknya bagi Masyarakat

Suku Dinas Komunikasi, Informatika dan Statistik - Jakarta Barat,

30 April 2026