

Cyber Security Awareness

Dark Web : Mengungkap Sisi Tersembunyi Internet & Dampaknya bagi Masyarakat

Suku Dinas Komunikasi, Informatika dan Statistik - Jakarta Barat,

30 April 2026



Disclaimer

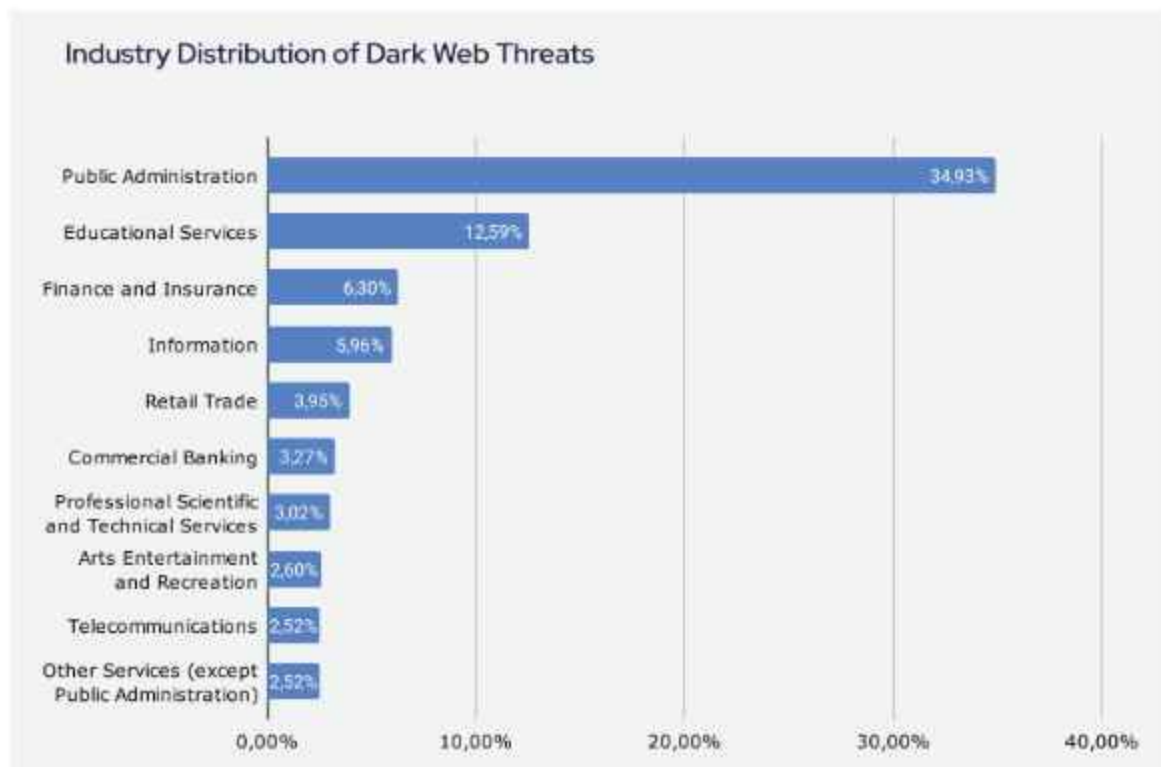
- Materi ini dibuat untuk tujuan edukasi dan kesadaran keamanan siber, bukan untuk mengajarkan atau mendorong aktivitas ilegal.
- Seluruh contoh dan tangkapan layar ditampilkan semata-mata untuk menggambarkan ancaman nyata yang ada di dunia siber.
- Informasi dalam materi ini tidak dimaksudkan sebagai 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.

Indonesia Threat Landscape

Jakarta Barat - 30 April 2026



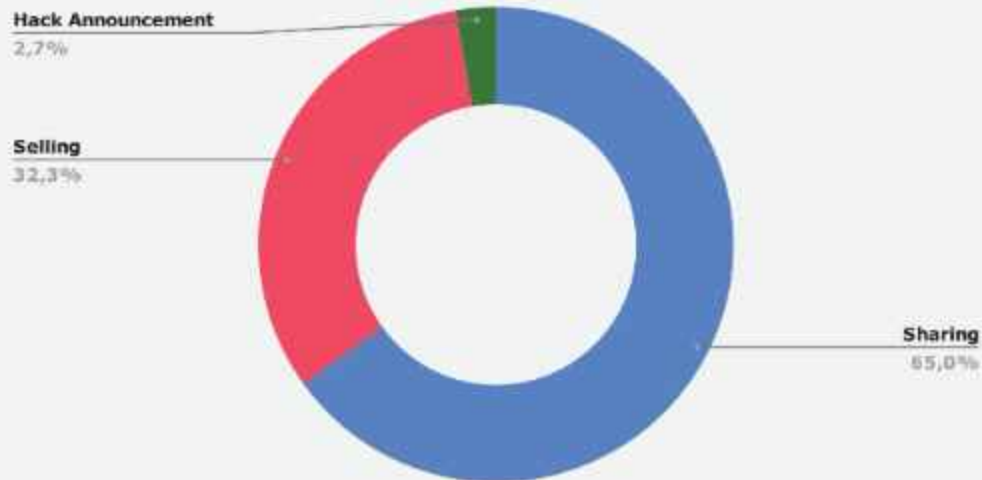
Indonesia Threat Landscape



Sumber: Indonesia Regional Threat Landscape Report 2025 - SOC RADAR

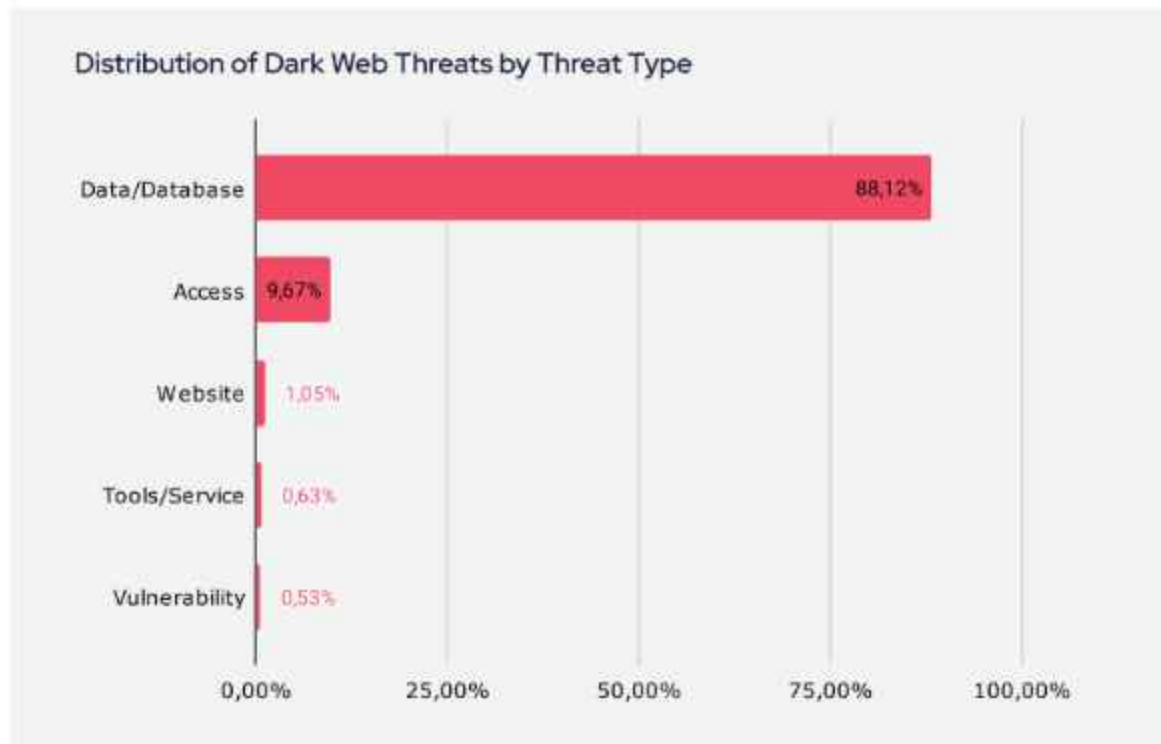
Indonesia Threat Landscape

Distribution of Dark Web Threats by Threat Categories



Sumber: Indonesia Regional Threat Landscape Report 2025 - SOC RADAR

Indonesia Threat Landscape

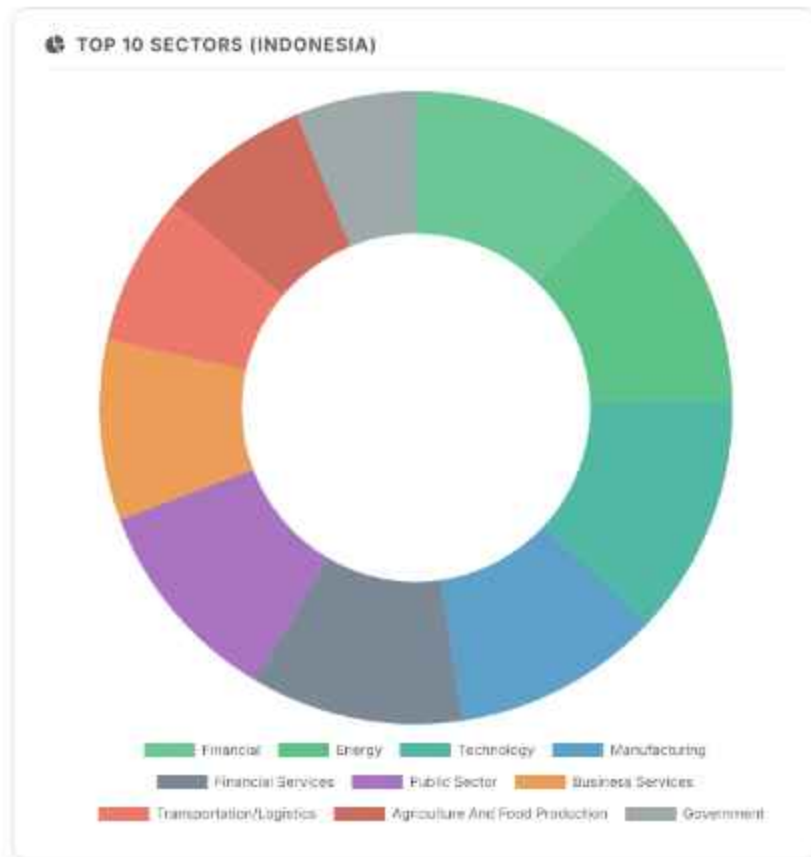


Sumber: Indonesia Regional Threat Landscape Report 2025 - SOC RADAR

Indonesia Threat Landscape

TOTAL VICTIMS
117
in Indonesia

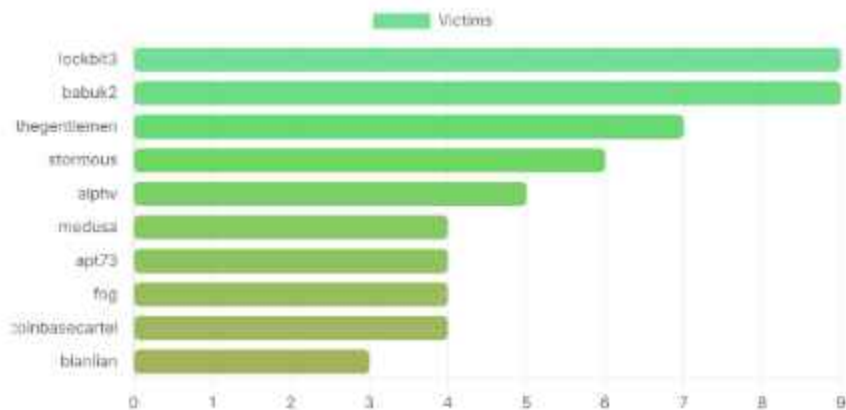
Sumber: transisi.wiki



Indonesia Threat Landscape

GROUPS INVOLVED
48
in Indonesia

🏠 TOP 10 GROUPS (INDONESIA)



Indonesia Threat Landscape

INFOSTEALERS WEEKLY REPORT

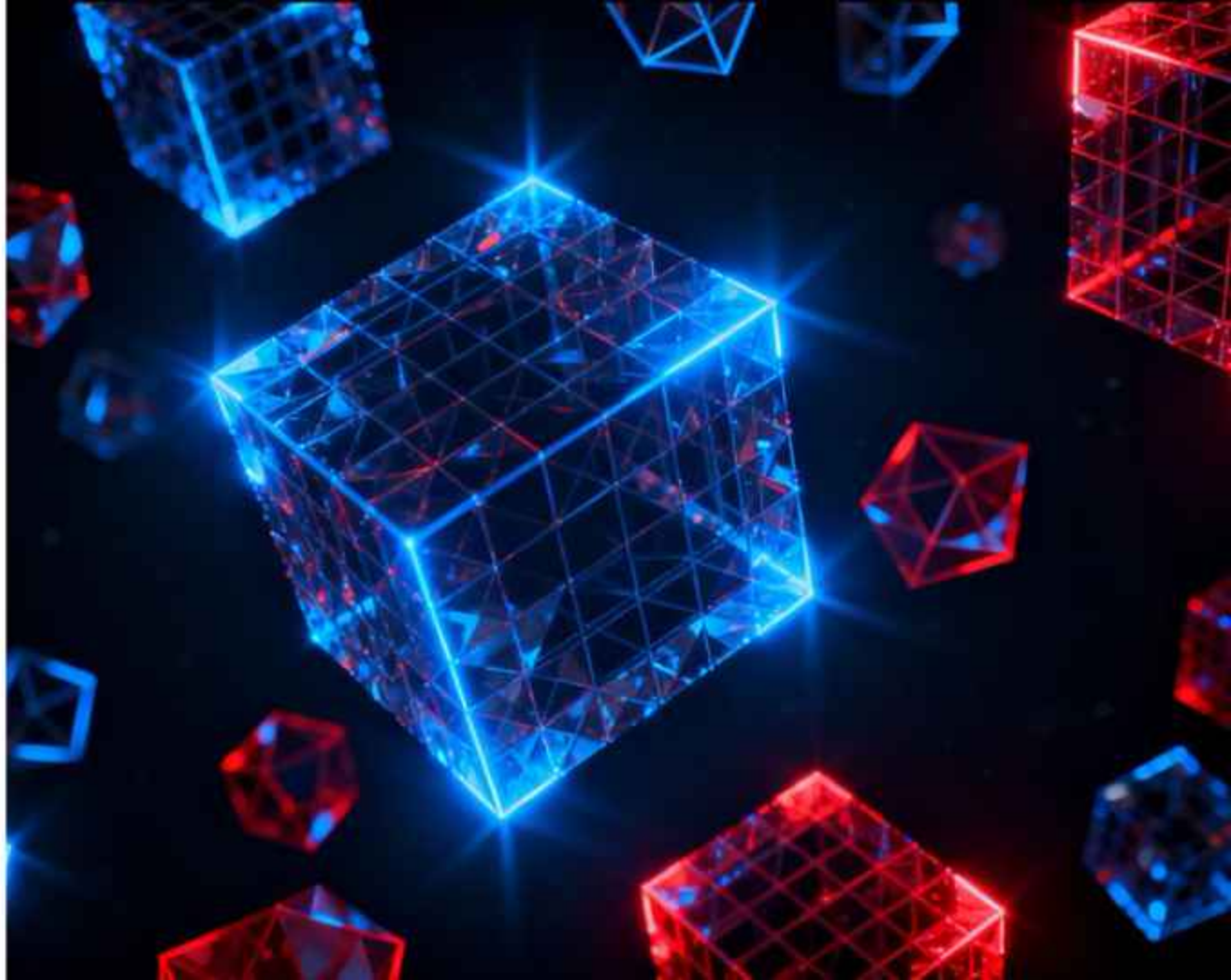
2026-04-20 - 2026-04-27



Sumber: InfoStealers - Huben Root

Struktur Internet & Area di Dalamnya

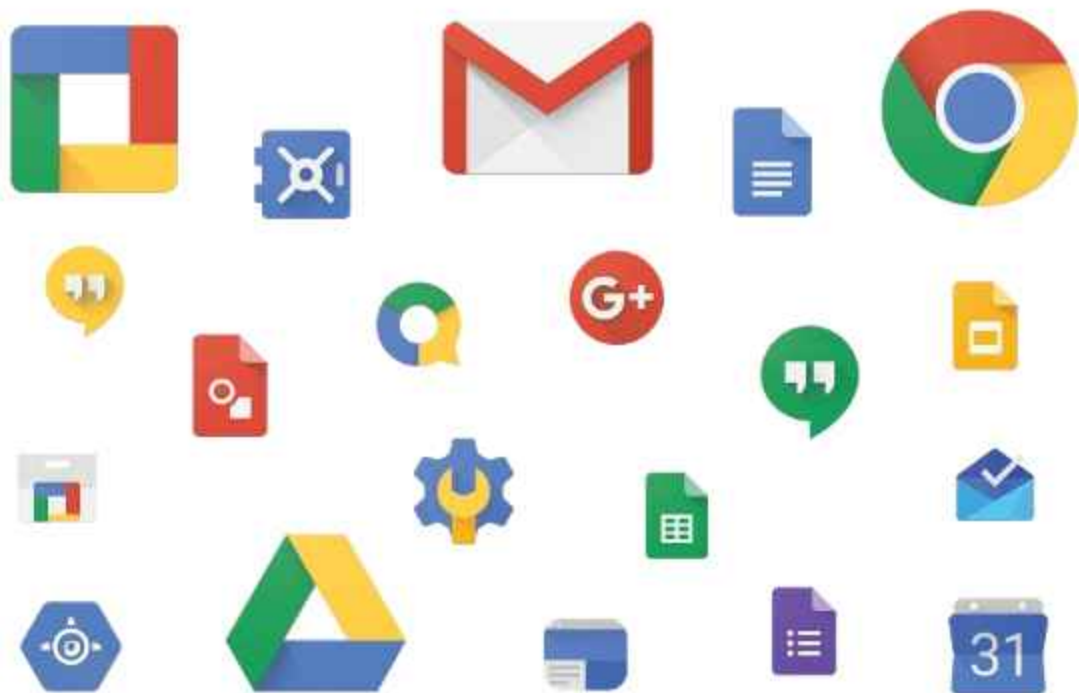
30 April 2026



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

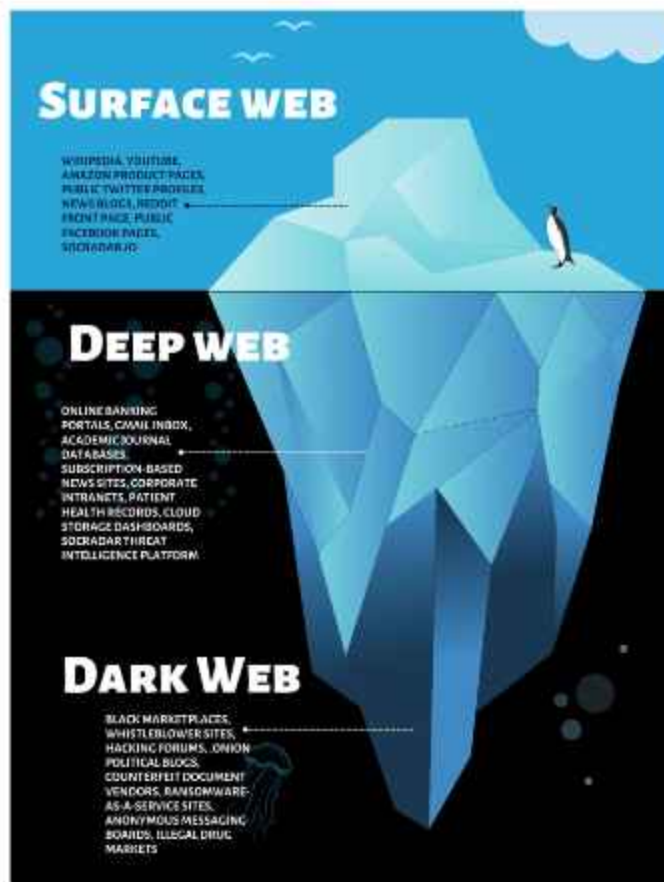
Private

- 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



Contoh Surface Web :

- Situs berita
- Blog
- Toko online
- Media sosial

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

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

Struktur Internet & Area di Dalamnya



Contoh Deep Web :

- Internet banking
- Database perusahaan
- Rekam medis
- Email

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

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.

Dark Web

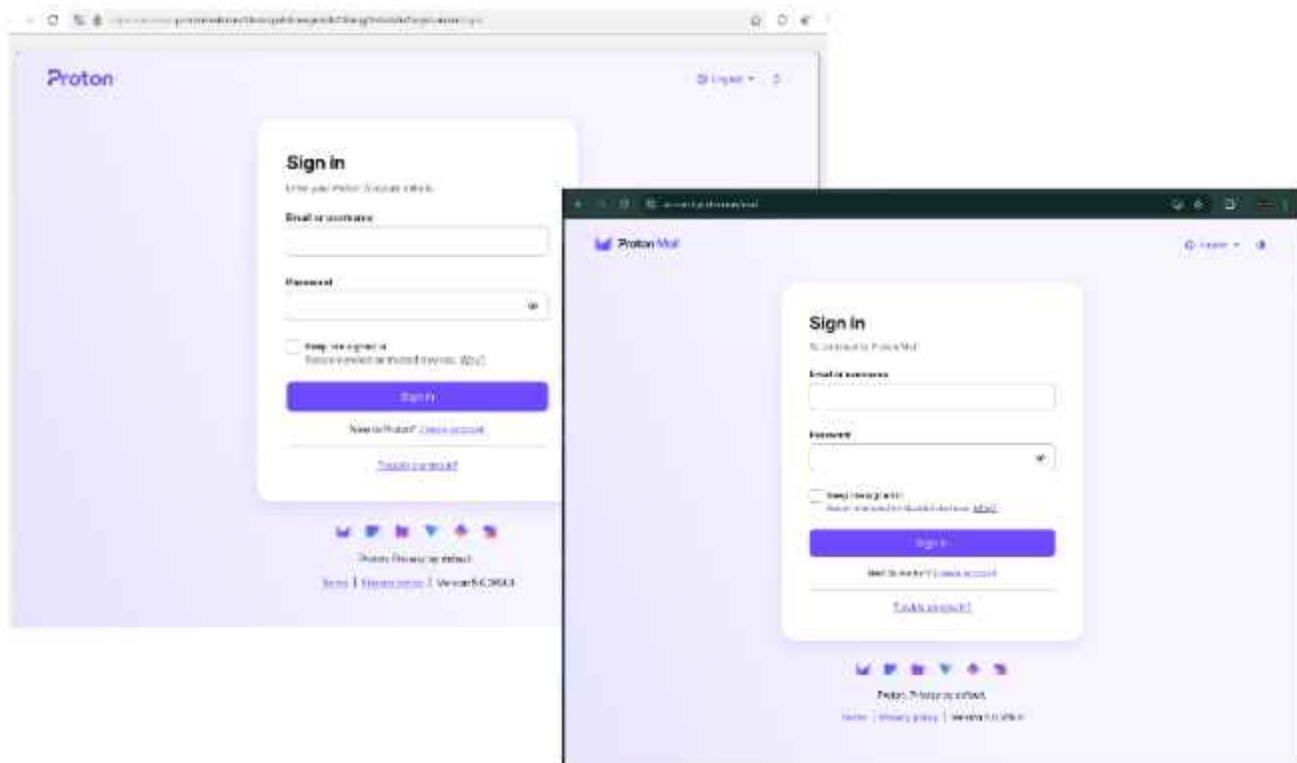
30 April 2026



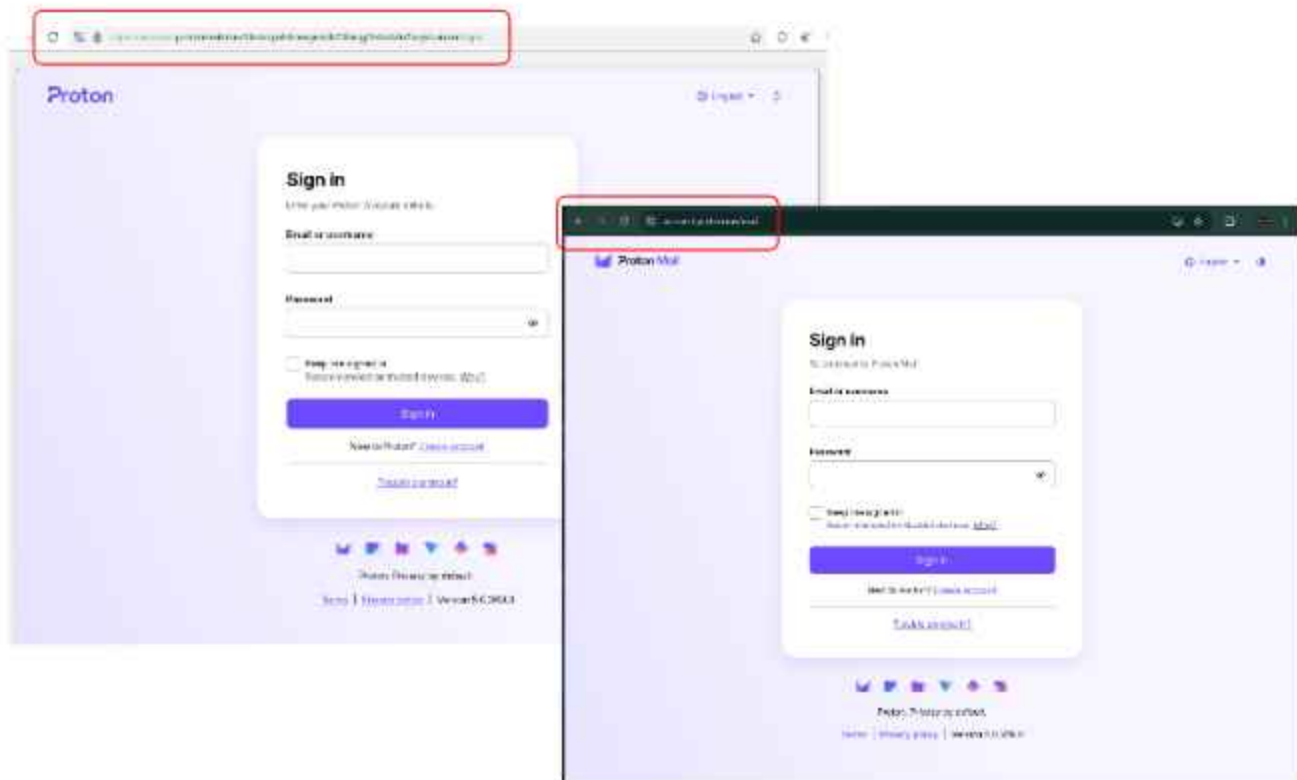
Dark Web

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.**

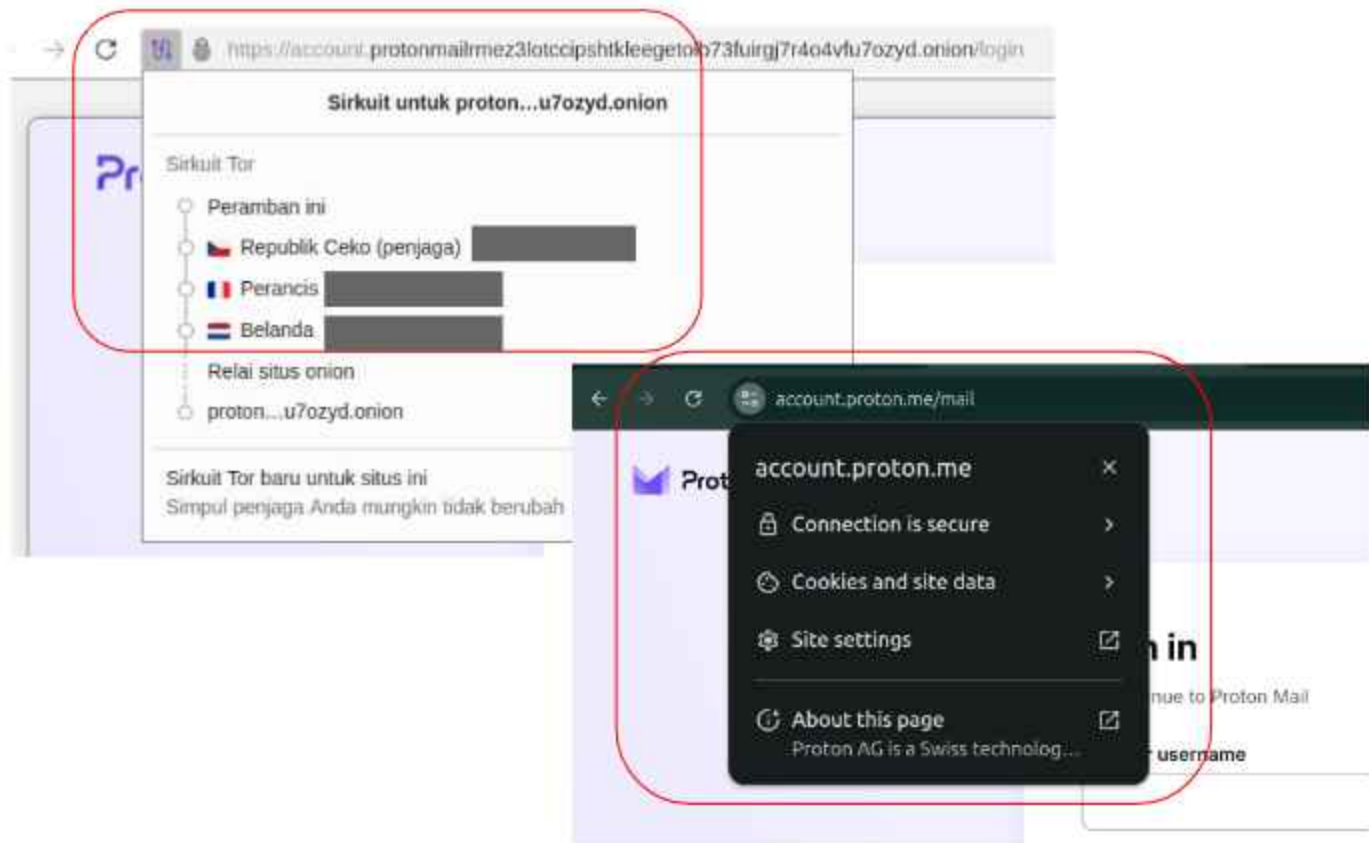
Dark Web



Dark Web



Dark Web



Dark Web

Dark Web tidak selalu identik dengan aktivitas ilegal

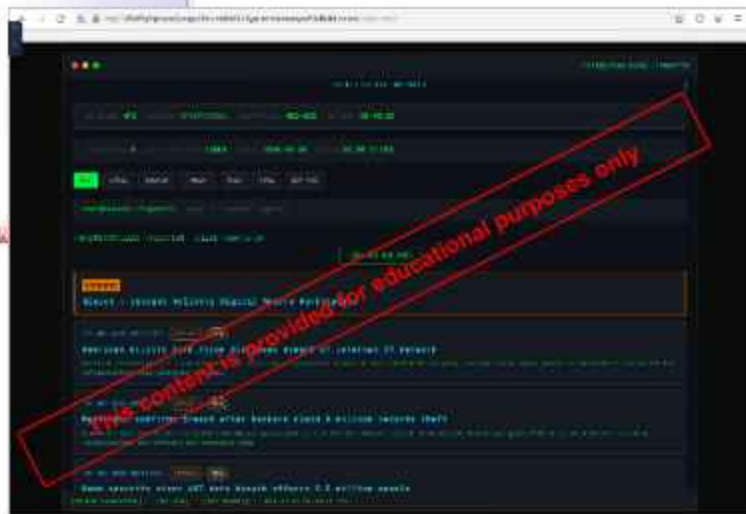
Teknologi ini dirancang untuk memberikan **privasi** dan **anonimitas** bagi penggunanya.

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



This content is provided for educational purposes only

Penyalahgunaan di Dark Web

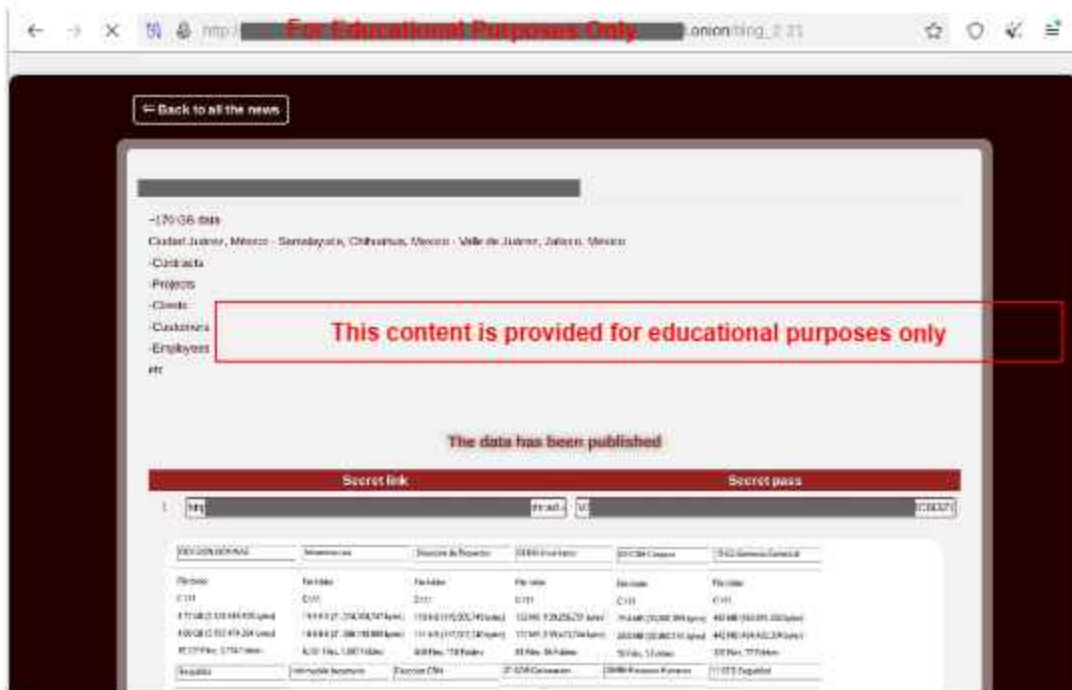
Dark Web



This content is provided for educational purposes only

Penyalahgunaan di Dark Web

Dark Web



This content is provided for educational purposes only

Penyalahgunaan di Dark Web

Dark Web

FOI Educational Purposes Only

ee.id 236 GB Database

Volume: 236.38 GB | 58,527 files | 6,402 documents

7. Identifiers of 1,500-1,700 employees file records

3,100 files scans of government-issued identity documents (KTP/KIK) containing photographs, national identification numbers linked to home addresses and dates of birth. The documents also contain hit data of employees' spouses, children and parents.

Additionally, 13,880 personal photographs, including a collection of FOTO PEGAWAI SYARAT JABATAN folder (1:32-Bes) linked to employee consistency profiles.

2. 743 personal mobile phone numbers

4 registry files personal numbers linked to each employee's full name, position, department and direct supervisor. Logarit file no: RP Pegawai Lask 8.24 WA.

3. 349 blood type records

12 master employee database files (RHP) registers versions RLV 4 / RLV 5 / RLV 6 and derivatives' medical data classified as a special category under UU PDP No. 27/2022 (Art. 4(2)(e)).

4. Classified dossier of the crime solver investigation material prepared for advisor: Wolff, Hans-Dieter

78 files psychometric profiles of each of the 72 SYPS, 38 VPS and 21 files: Mh, petramasasa indeks, larang, kategori, JA / JI / J2 / J3, ASI attachment card conclusions with recommendations of "approved / not recommended"

Nonpublic personnel evaluations of the level of the Ministry of State-Owned Enterprises.

5. 141 psychological profiles of 200+ executives

28 files (within the Directorate dossier package) 29 competencies, Big Five, SMART personality profile with dedicated "Strengths" and "Areas for Development" sections for each member of the management hierarchy.

6. Composite of the payroll and HR system

45 salary and payment documents files credentials and access linking to the corporate payroll system. Bank account details and complete payment history of the folder for 2022-2025.

7. Employees of strategic facilities with tax identification numbers and home addresses.

This content is provided for educational purposes only

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

Jawa Plus
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



HOME ▾ KEPRI ▾ EKONOMI ▾ NASIONAL ▾ TN POLRU ▾ POLITIK ▾ WARTARE

Siapa Saja **Cerita**

OJK Kepri Waspada Lonjakan Kejahatan Siber, Ribuan Kasus Penipuan Terungkap

08:00 WIB - 08:00 WIB

TEMPO

Menu Hariin Minggu

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.

1 Maret 2026 | 22:34 WIB

Dampak pada Masyarakat



Dampak pada Masyarakat

co.id 236 GB DataBase

Volume: 236 58 GB | 58,537 files | 6,402 directories

1. Identities of 1,500-1,700 employees fully exposed
3,100 files scans of government-issued identity documents (KTP/KK) containing photographs, national identification numbers (NIK), home addresses and dates of birth. The repository also contains NIK data of employees' spouses, children and parents.

Additionally, 15,993 personnel photographs, including a dedicated FOTO PEGAWAI SYARAT JABATAN folder (1,132 files) linked to position competency profiles.

2. 793 personal mobile phone numbers
4 registry files personal numbers linked to each employee's full name, position, department and direct supervisor.
Largest file: No HP Pegawai 1.xlsx 9.24 MB.

3. 569 blood type records
12 master employee database files (ERP registries versions REV 4 / REV 5 / REV 6 and derivatives) medical data classified as a special category under UU PDP No. 27/2022 (Art. 4(2)(a)).

4. Classified dossiers on the entire senior management materials prepared for sovereign wealth fund Danantara
36 files psychometric profiles of each of the 13 SVPs, 58 VPs and 31 AVPs; MKI performance indices, talent categories (A / B1 / B2 / B3), ASI assessment center conclusions with recommendations of "approved / not recommended".

Non-public personnel evaluations at the level of the Ministry of State-Owned Enterprises.

5. Full psychological profiles of 200+ executives
36 files (within the Danantara dossier package) 26 competencies, Big Five, SMART personality profile with dedicated "Strengths" and "Areas for Development" sections for each member of the management hierarchy.

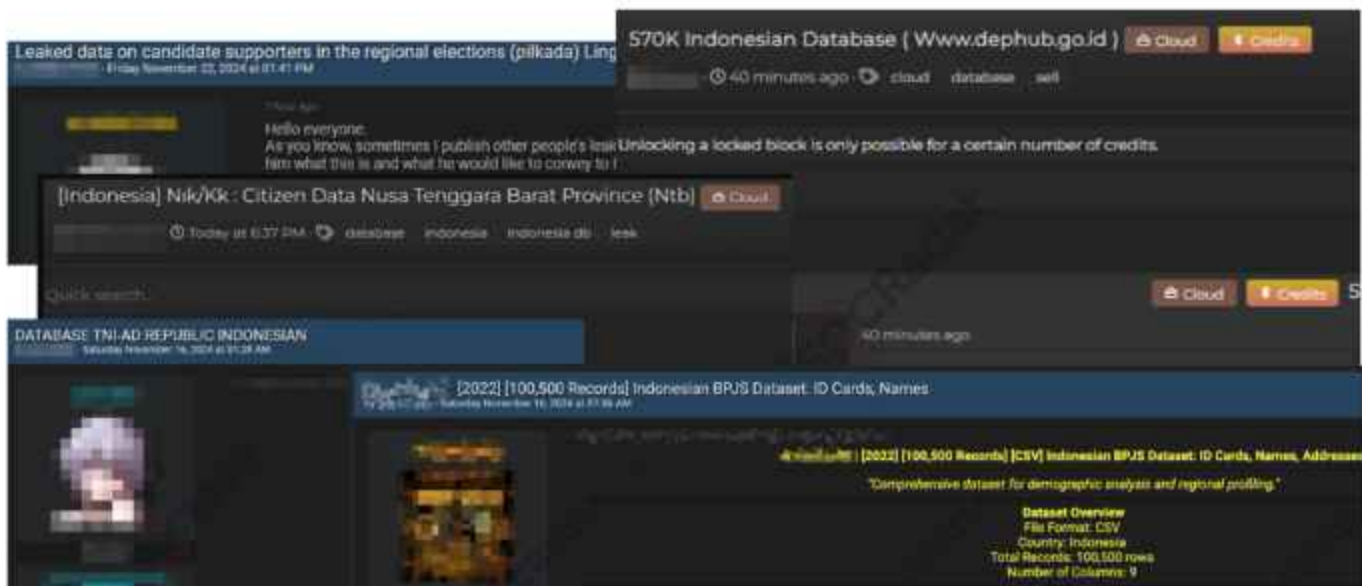
6. Compromise of the payroll and ERP system
45 payroll and payment document files credentials and access tokens to the corporate payroll system; Bank account details and complete payment history of the insider for 2022-2025.

7. Employees of strategic facilities with tax identification numbers and home addresses.



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

Dampak pada Masyarakat



Dampak pada Masyarakat



Dampak pada Masyarakat

```

1 SOFT: Chrome Default (129.0.6668.70)
2 URL: https://www.facebook.com/
3 USER: [REDACTED]
4 PASS: [REDACTED]
5
6 SOFT: Chrome Default (129.0.6668.70)
7 URL: https://www.facebook.com/
8 USER: [REDACTED] l.com
9 PASS: [REDACTED]
10
11 SOFT: Chrome Default (129.0.6668.70)
12 URL: https://signin.oracle.com/signin
13 USER: [REDACTED]
14 PASS: [REDACTED]
15
16 SOFT: Edge Default (129.0.2792.65)
17 URL: https://www.facebook.com/
18 USER: [REDACTED] l.com
19 PASS: [REDACTED]
20
21 SOFT: Edge Default (129.0.2792.65)
22 URL: https://signin.oracle.com/signin
23 USER: [REDACTED]
24 PASS: [REDACTED]
25
26 SOFT: Mozilla Firefox
27 URL: https://www.facebook.com
28 USER: [REDACTED]
29 PASS: [REDACTED]
30
31 SOFT: Mozilla Firefox
32 URL: https://www.noon.com
33 USER: [REDACTED]
34 PASS: [REDACTED]
35
36 SOFT: Mozilla Firefox
37 URL: https://accounts.google.com
38 USER: [REDACTED]
39 PASS: [REDACTED]

```

```

1 Password Entry: URL: [REDACTED] pc.id/
2 Password Username: [REDACTED]
3 User Information:
4 Mail ID: [REDACTED]
5 IP: [REDACTED]
6 FileLocation: C:\Windows\Microsoft.NET\Framework\v4.0.30319\wpaes0hps.exe
7 UserName: [REDACTED]
8 MachineName: [REDACTED]
9 Country ID: [REDACTED]
10 Zip Code: 17108
11 Location: Bekasi, Jawa Barat
12 WWD: [REDACTED]
13 Current Language: English (United States)
14 ScreenSize: (width=1029, height=1800)
15 TimeZone: (UTC+07:00) Bangkok, Hanoi, Jakarta
16 Operation System: Windows 10 Home Single Language x64
17 Log date: 7/20/2024 14:53:39
18 Available KeyboardLayouts:
19 English (United States)
20 Hardware:
21 Name: Total of RAM, 16383.77 MB or 17815699648 bytes
22 Name: Intel(R) Core(TM) i7-7700HQ CPU @ 2.80GHz, 4 Cores
23 Name: Intel(R) HD Graphics 630, 1873741824 bytes
24 Name: NVIDIA GeForce GTX 1060, 322125472 bytes
25 Anti-Virus:
26 Windows Defender
27 360 Total Security
28
29
30 Password Entry: URL: [REDACTED] pc.id/register
31 Password Username: [REDACTED]
32 User Information:
33 Mail ID: [REDACTED]
34 IP: [REDACTED]
35 FileLocation: C:\Windows\Microsoft.NET\Framework\v4.0.30319\2mlr8qj\CT4.exe
36 UserName: [REDACTED]
37 MachineName: [REDACTED]
38 Country ID: [REDACTED]
39 Zip Code: 12884
40 Location: Jakarta, Jakarta Raya
41 WWD: [REDACTED]
42 Current Language: English (Indonesia)
43 ScreenSize: (width=1029, height=1800)
44 TimeZone: (UTC+07:00) Bangkok, Hanoi, Jakarta
45 Operation System: Windows 11 Pro x64
46 Log date: 7/29/2024 14:58:43
47 Available KeyboardLayouts:
48 English (Indonesia)
49 English (United States)
50 Hardware:
51 Name: Total of RAM, 12221.12 MB or 128167552e bytes
52 Name: Intel(R) Pentium(R) CPU G3348 @ 3.19GHz, 3 Cores
53 Name: AMD Radeon R9 380 Series, 1873741824 bytes
54 Anti-Virus:
55 Windows Defender

```

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, Ifan Maulana
Tin Redaksi



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

The screenshot shows the top portion of a news article on the Kompas.com website. At the top, the navigation bar includes the site logo 'KOMPAS.com' and various category links: News, Kolom, Event, Cahaya, Tekno, Otomotif, Bola, Lifestyle, Tren, Lestari, Money, Properti, Edukasi, and Travel. Below the navigation bar, there are social media sharing icons for Facebook, X, WhatsApp, and Telegram, followed by the article title 'Komdigi: 60 Persen Pengguna Seluler Terima "Spam Call" Minimal Satu Minggu Sekali' and a 'KOMENTAR:' link. The main content area features the breadcrumb 'Kompas.com / News / Nasional', the full article title, the publication date and time 'Kompas.com, 27 Januari 2026, 20:16 WIB', and a row of utility icons including a thumbs up, 'Add on Google', a trash can, a share icon, a comment icon, and a bookmark icon. At the bottom left, there is a circular profile picture with the initials 'FRB' and the author's name 'Firda Janati, Robertus Belarminus' with the role 'Tim Redaksi' below it.

Dampak pada Masyarakat



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

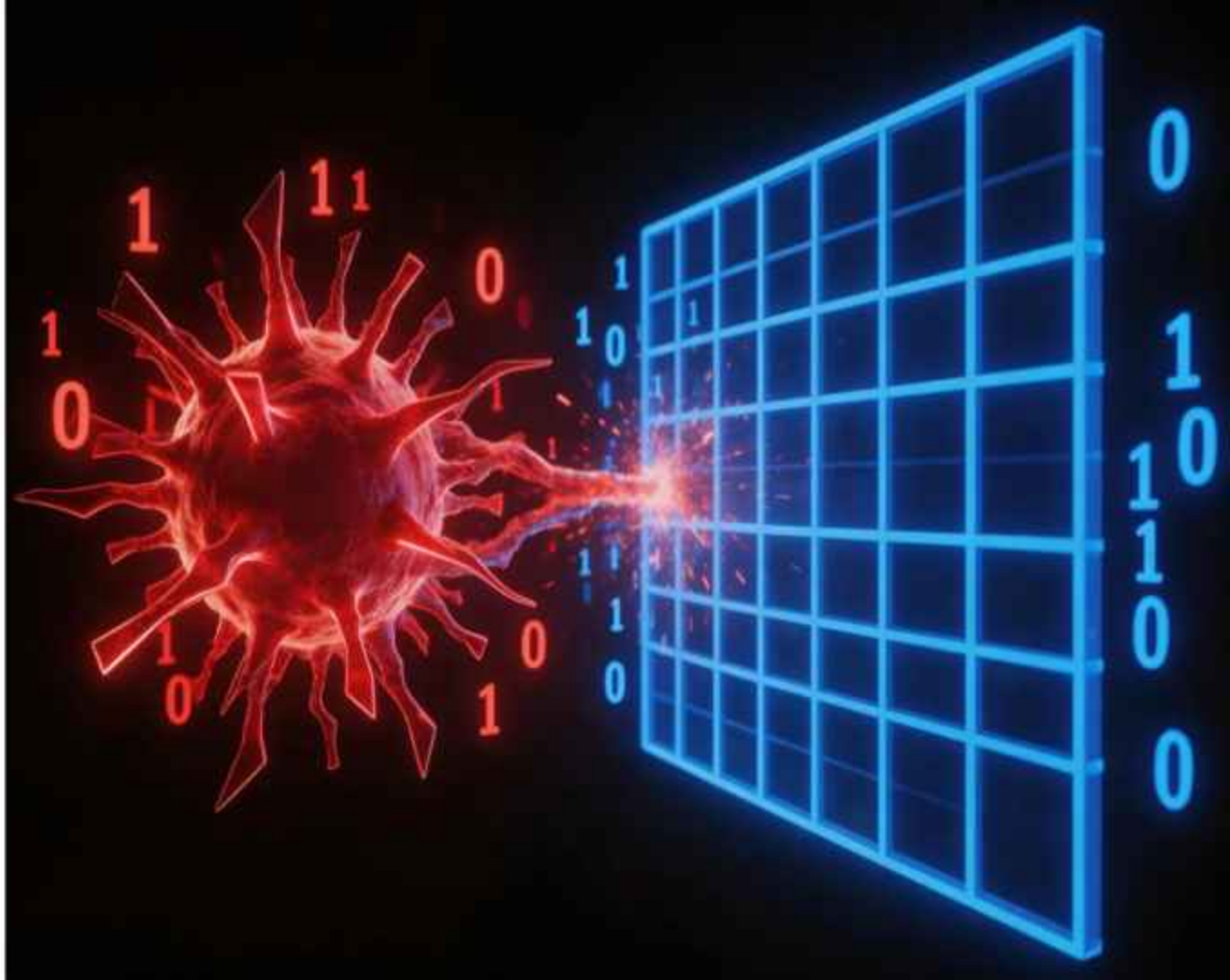
Aspek Hukum

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

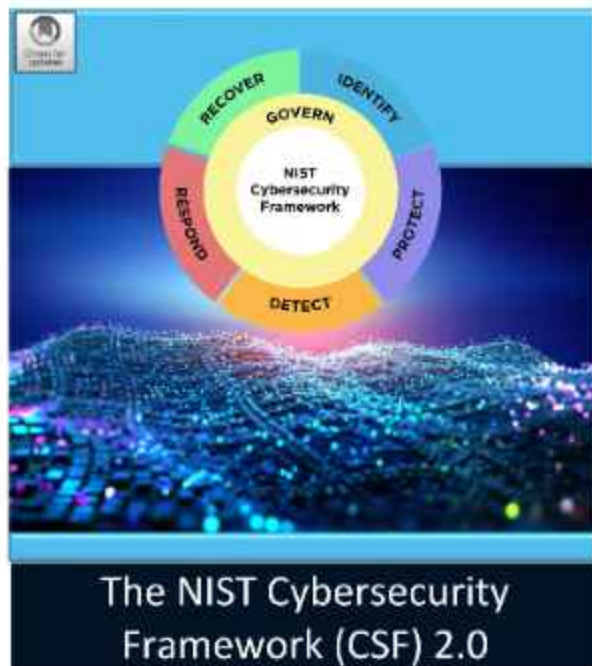
Mengetahui aturan adalah **bagian dari kontribusi** kita menjaga keamanan digital bersama.

Standar Keamanan

30 April 2026



Standar Keamanan



National Institute of Standards and Technology
This publication is available free of charge from: <https://doi.org/10.6028/NIST.CSSP.20>
February 20, 2024

NIST NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

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



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



Standar Keamanan

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

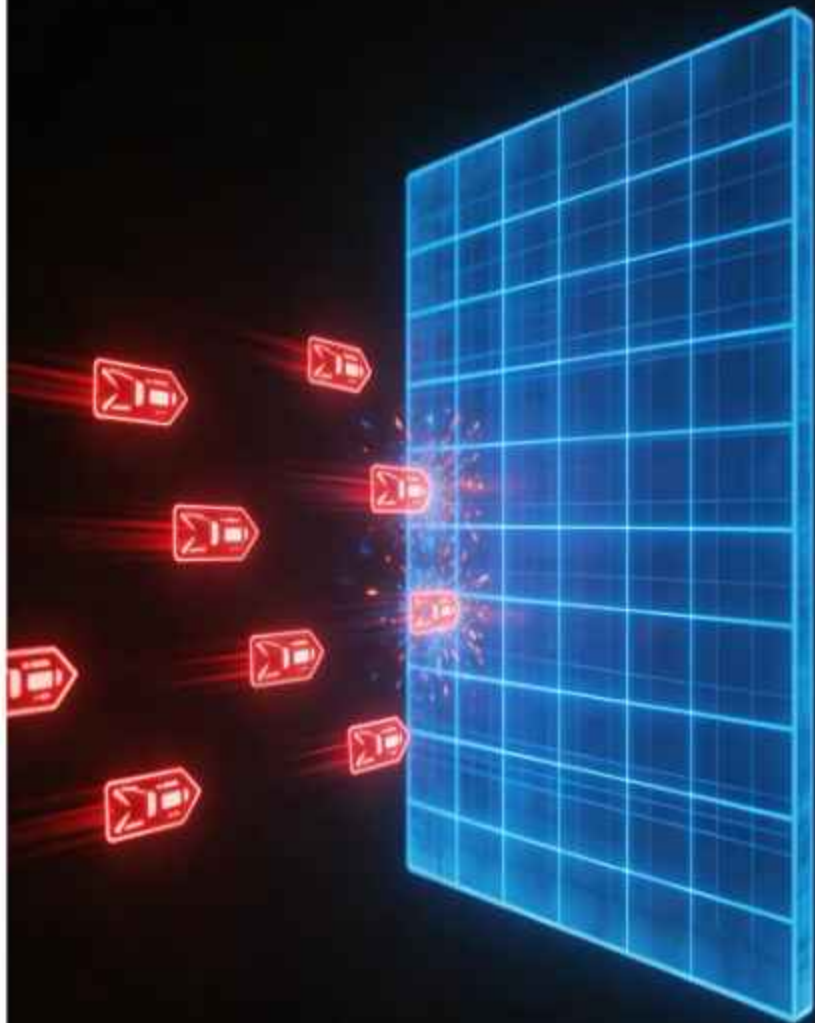


Regulasi Bank Indonesia yang mengatur penerapan keamanan sistem informasi dan ketahanan siber bagi penyelenggara sistem pembayaran, pelaku pasar uang dan pasar valuta asing, serta pihak lain yang diawasi Bank Indonesia. Ruang lingkup pengaturan mencakup :

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

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

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

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 & PRAA-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.

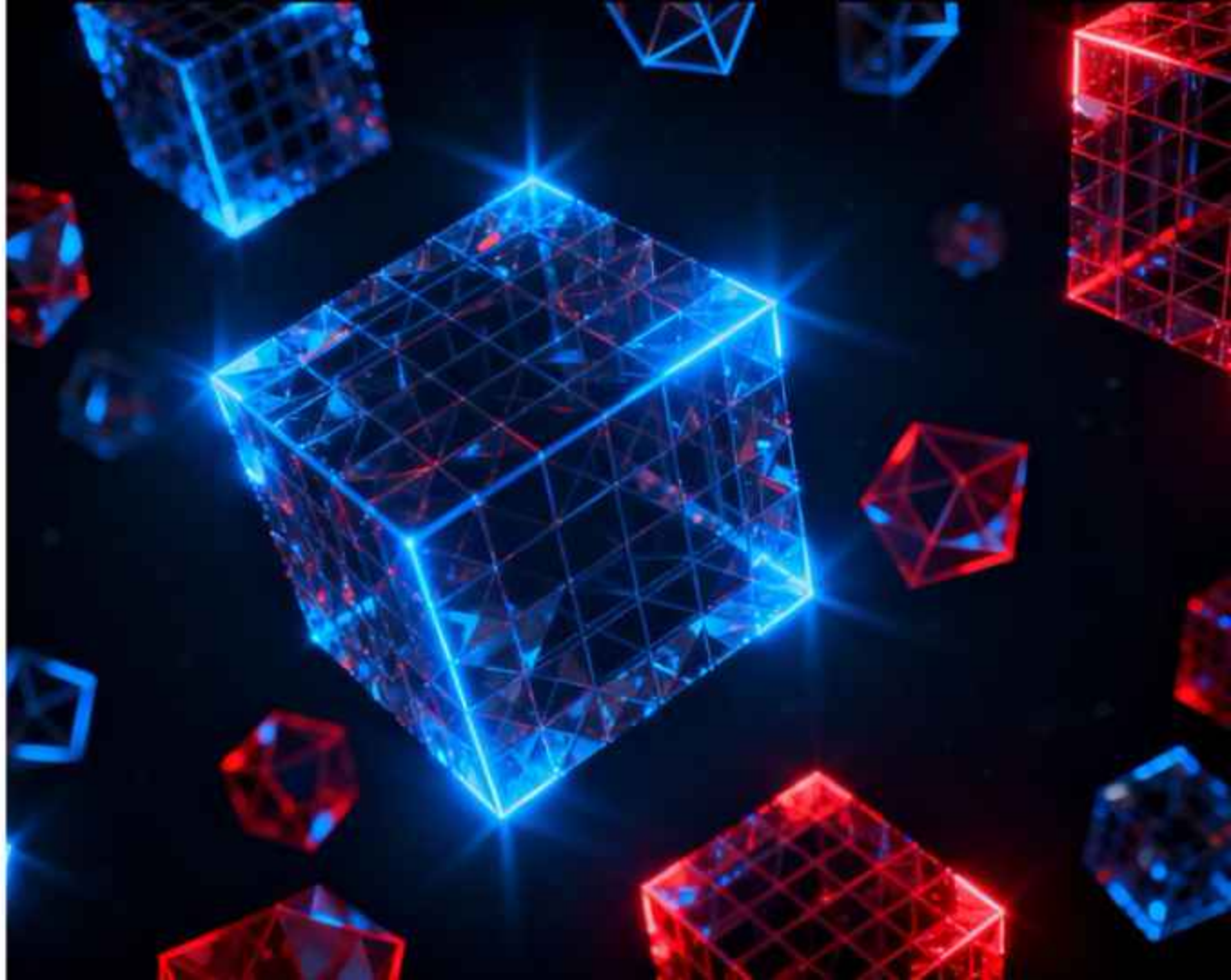
Referensi : ISO 27001:2022 – A.8.16 Pemantauan aktivitas | NIST CSF 2.0 – DE.CM-03

- **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

Kontribusi Bersama

30 April 2026



Kontribusi Bersama

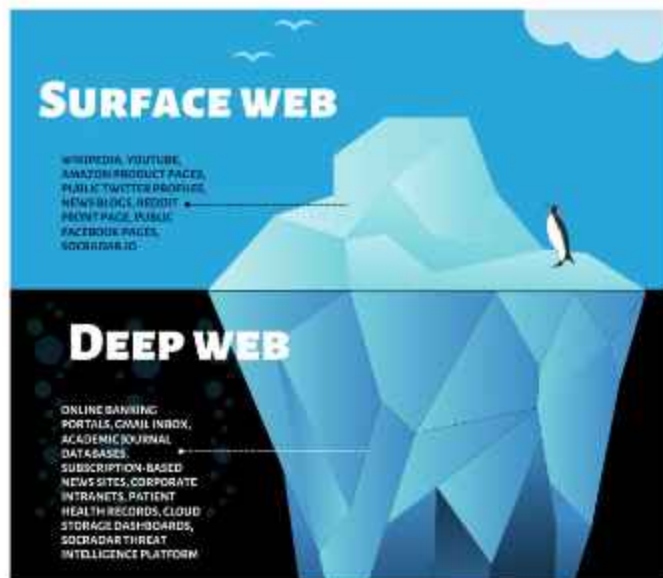
Keamanan siber bukan hanya tanggung jawab organisasi atau penyedia layanan, tetapi juga menjadi **tanggung jawab bersama** sebagai pengguna internet.

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

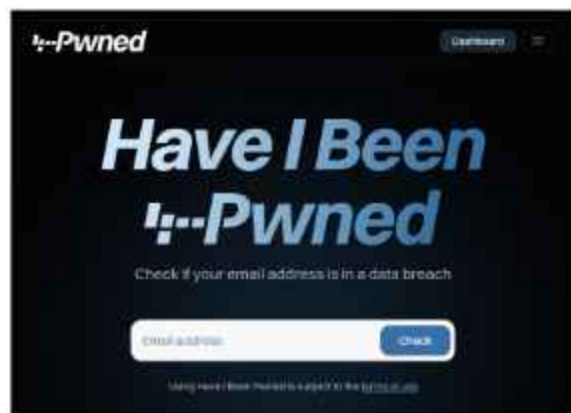


DON'T



Kontribusi Bersama

DO



DON'T



Kontribusi Bersama

DO

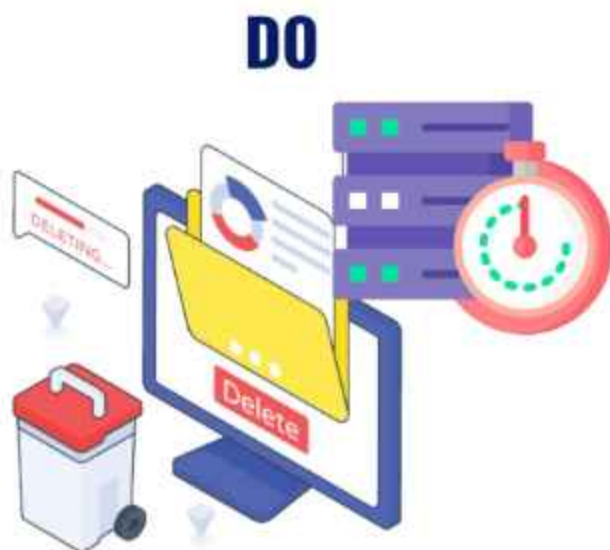
The image shows two side-by-side screenshots of privacy notices. On the left is the AWS Privacy Notice, last updated May 12, 2021. On the right is the Google Cloud Privacy Notice. Both pages contain detailed text about data collection, processing, and user rights.

DON'T

The image shows a screenshot of the Tokopedia website search results for 'vps murah'. The page displays a grid of VPS products with their prices and specifications.

Produk	Rating	Harga	Spesifikasi
VPS Windows Ultra ...	4.0 - 27 ulasan	Rp39.777	OS: Windows 10
EA Trading Cloud E10...	4.5 - 100+ ulasan	Rp20.000	RAM: 1GB - 16GB, SSD: 10GB
VPS Instan target...	4.0 - 2 ulasan	Rp50.000	RAM: 4GB, SSD: 10GB
VPS Linux v2 Cara ...	4.0 - 1 ulasan	Rp50.000	RAM: 4GB, SSD: 10GB

Kontribusi Bersama



DON'T



Kontribusi Bersama

DO



DON'T



Kontribusi Bersama

DO



DON'T

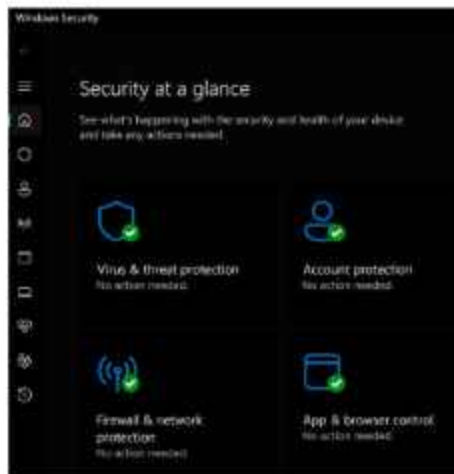
PERINGATAN

Download WPS Office Full Crack Bagas31 Terbaru 2026

APRIL 19, 2026

Kontribusi Bersama

DO



DON'T



Kontribusi Bersama

DO

Contoh 1:

Contoh: email@tikopedia.com

Daftar

Dengan mendaftar, saya menyetujui Syarat & Ketentuan serta Kebijakan Privasi Tokopedia.

Contoh 2:

Contoh: email@tikopedia.com

Daftar

Dengan mendaftar, saya menyetujui Syarat & Ketentuan serta Kebijakan Privasi Tokopedia.

DON'T

Contoh 1:

Contoh: email@tikopedia.com

Daftar

Dengan mendaftar, saya menyetujui Syarat & Ketentuan serta Kebijakan Privasi Tokopedia.

Contoh 2:

Contoh: email@tikopedia.com

Daftar

Dengan mendaftar, saya menyetujui Syarat & Ketentuan serta Kebijakan Privasi Tokopedia.

Kontribusi Bersama

DO



DON'T



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-hidytlah

Terimakasih

Dark Web : Mengungkap Sisi Tersembunyi Internet & Dampaknya bagi Masyarakat

Suku Dinas Komunikasi, Informatika dan Statistik - Jakarta Barat,
30 April 2026
