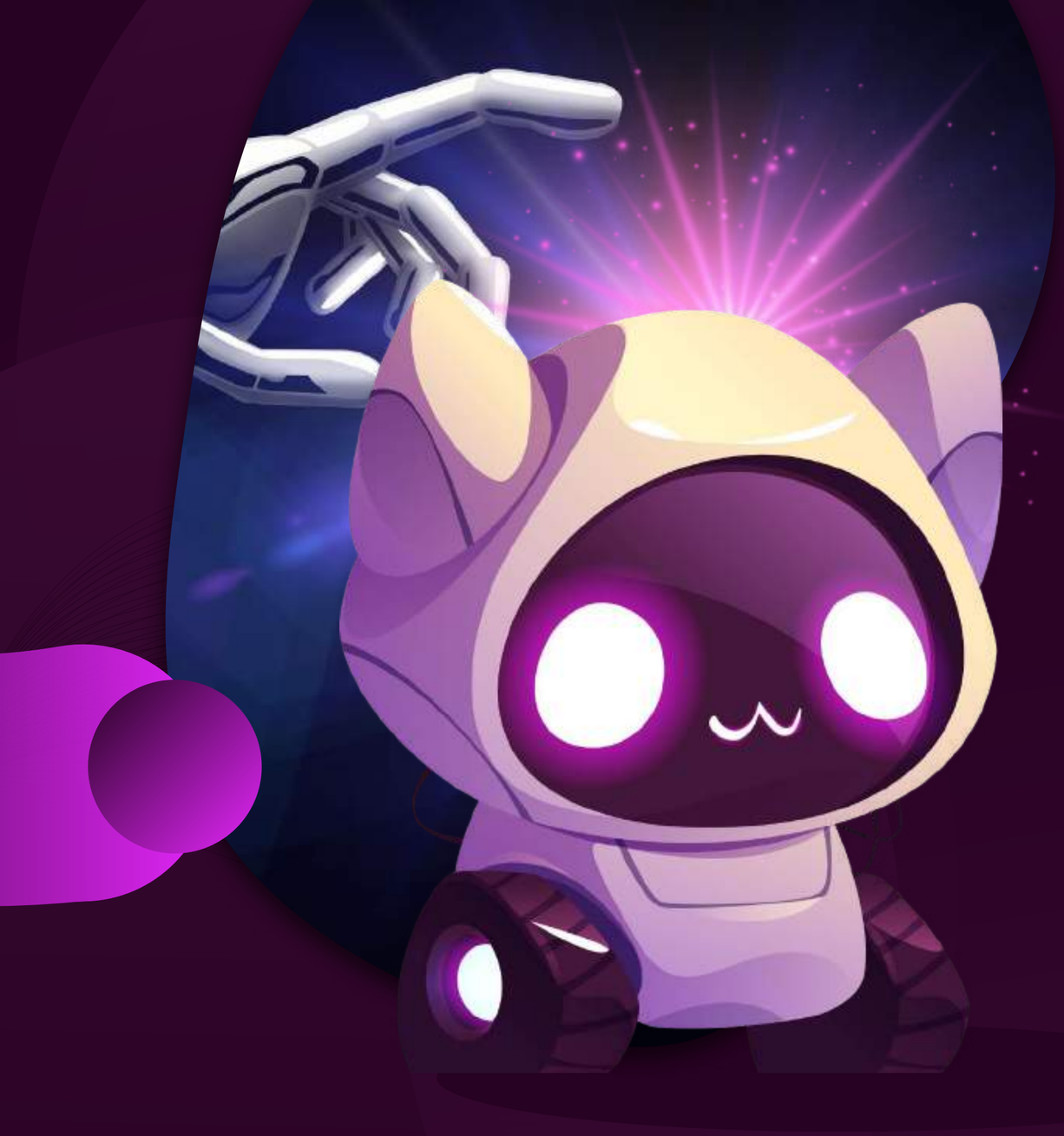
{ Cyber.b1te }



# ETIKA & KEPATUHAN KEAMANAN SIBER

Memahami regulasi keamanan digital, kebijakan organisasi, dan tanggung jawab individu dalam dunia maya.

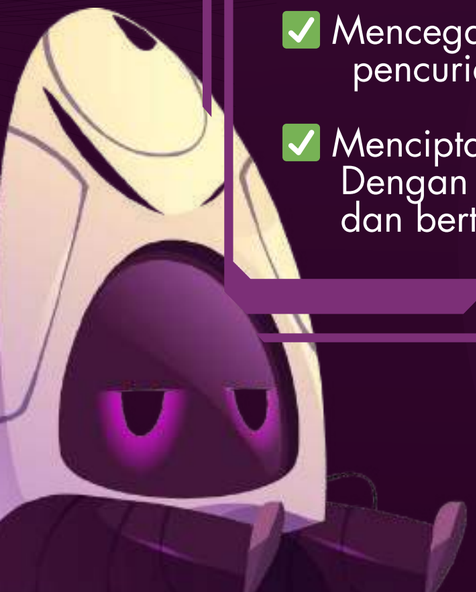
{ Cyber.b1te }

# Pendahuluan

Keamanan digital bukan hanya tentang teknologi, tetapi juga tentang kepatuhan hukum dan tanggung jawab individu.

## Mengapa ini penting?

- ✅ Perlindungan data pribadi – Agar informasi sensitif tidak disalahgunakan.
- ✅ Mencegah kejahatan siber – Seperti peretasan, pencurian data, dan penipuan online.
- ✅ Menciptakan lingkungan digital yang sehat – Dengan menggunakan media sosial secara bijak dan bertanggung jawab.



## Modul ini membahas

1. Regulasi hukum yang mengatur keamanan digital.
2. Kebijakan organisasi dalam melindungi data.
3. Peran individu dalam menjaga keamanan dan etika digital.

{ Cyber.b1te }

# HUKUM & REGULASI TERKAIT KEAMANAN SIBER

Setiap negara memiliki regulasi untuk melindungi pengguna dari ancaman siber.

## GDPR (General Data Protection Regulation)

- Regulasi ketat yang mengatur perlindungan data pribadi.
- Setiap perusahaan harus meminta izin sebelum mengumpulkan data pengguna.
- Pelanggaran bisa didenda hingga €20 juta atau 4% dari pendapatan tahunan global.

## UU ITE (Undang-Undang Informasi dan Transaksi Elektronik)

- Melindungi transaksi elektronik dan privasi pengguna.
- Mengatur sanksi bagi pelaku kejahatan siber, termasuk penyebaran hoaks dan pencurian data.
- Pelanggaran bisa dikenakan denda hingga Rp10 miliar atau hukuman penjara.

## CCPA (California Consumer Privacy Act)

- Memberikan hak kepada warga untuk mengetahui bagaimana data mereka digunakan.
- Memungkinkan pengguna meminta penghapusan data mereka dari perusahaan.

# PELANGGARAN & KONSEKUENSI HUKUM

{ Cyber.b1te }

### Pencurian data pribadi

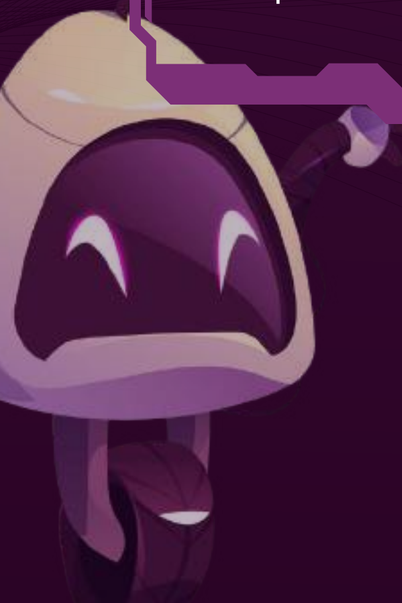
Hukuman denda dan penjara bagi pelaku yang mengambil atau menjual data tanpa izin.

### Serangan siber (hacking, phishing, ransomware)

Hukuman pidana yang berat bagi pelaku yang menyebabkan kerugian besar.

### Penyebaran hoaks & ujaran kebencian

Bisa dikenakan denda besar dan pemblokiran akun atau situs.



✅ Bagaimana agar kita tidak terjerat masalah hukum?

- ✓ Pahami hak dan kewajiban terkait data pribadi.
- ✓ Jangan menyebarkan informasi yang tidak terverifikasi.
- ✓ Hormati privasi orang lain dan patuhi kebijakan platform digital.

# KEBIJAKAN KEAMANAN DALAM ORGANISASI

{ Cyber.b1te }

📌 Langkah-langkah kebijakan keamanan dalam organisasi:

## Manajemen Kata Sandi & Akses Data

- Semua karyawan wajib menggunakan kata sandi yang kuat.
- Penerapan autentikasi dua faktor (2FA) di semua akun perusahaan.
- Prinsip least privilege, hanya orang yang berwenang yang bisa mengakses data tertentu.

## Enkripsi & Proteksi Data

- Semua data pelanggan dan perusahaan harus dienkripsi sebelum disimpan atau dikirim.
- Perusahaan harus memiliki backup data untuk mencegah kehilangan akibat serangan siber.

## Pelatihan Keamanan Siber untuk Karyawan

- Edukasi rutin tentang phishing, malware, dan social engineering.
- Simulasi serangan siber untuk meningkatkan kewaspadaan.

# TANGGUNG JAWAB PENGGUNA DALAM KEAMANAN DIGITAL

Setiap individu memiliki peran dalam menjaga keamanan digital.

🚨 Jika kita tidak berhati-hati, kita bisa menjadi korban kejahatan siber!

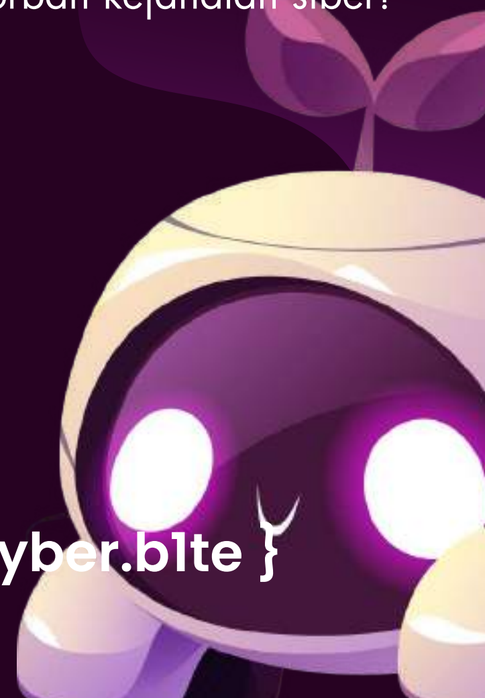
01 Gunakan kata sandi yang kuat & unik untuk setiap akun.

02 Aktifkan autentikasi dua faktor (2FA) di akun penting.

03 Jangan sembarangan membagikan informasi pribadi di internet.

04 Selalu verifikasi sumber informasi sebelum mengklik tautan atau mengunduh file.

05 Gunakan perangkat lunak antivirus yang selalu diperbarui.



{ Cyber.b1te }

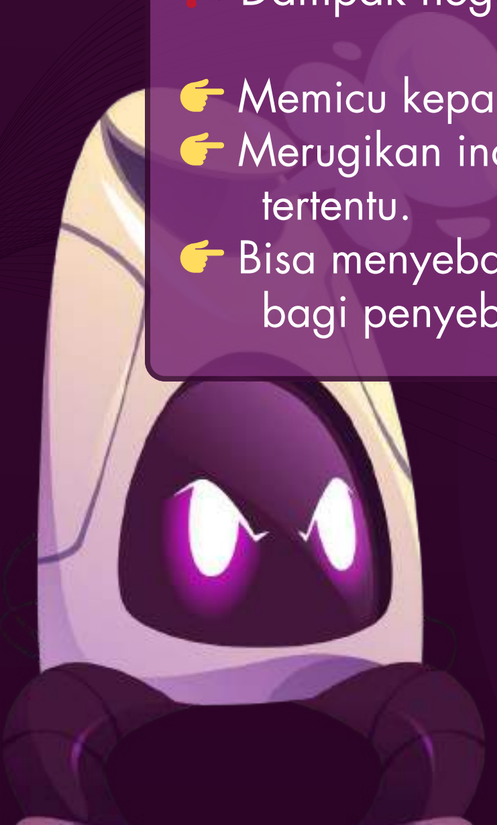
# MENGHINDARI PENYEBARAN HOAKS & INFORMASI PALSU

{ Cyber.b1te }

Hoaks adalah berita palsu atau informasi menyesatkan yang disebarkan untuk tujuan tertentu.

📢 Dampak negatif penyebaran hoaks:

👉 Memicu kepanikan dan konflik.
👉 Merugikan individu atau kelompok tertentu.
👉 Bisa menyebabkan konsekuensi hukum bagi penyebarnya.

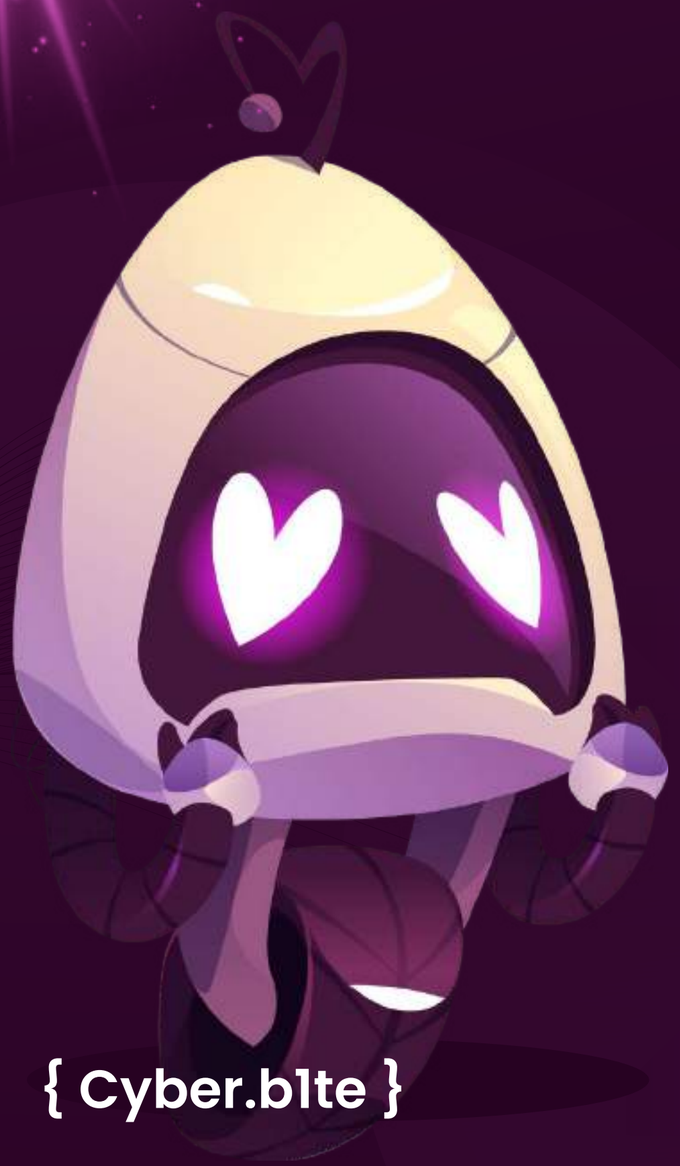


01 Selalu cek sumber berita sebelum membagikan informasi.

02 Verifikasi fakta melalui situs berita terpercaya atau layanan cek fakta.

03 Jangan mudah percaya pada pesan berantai tanpa bukti.

# MENGGUNAKAN MEDIA SOSIAL SECARA ETIS



{ Cyber.b1te }

- Hormati privasi orang lain.
- Jangan melakukan cyberbullying atau menyebarkan ujaran kebencian.
- Hati-hati saat membagikan foto atau informasi pribadi.
- Gunakan fitur keamanan media sosial seperti pengaturan privasi dan laporan konten.
- Bersikap sopan dalam diskusi online dan tidak memprovokasi.

# PRAKTIK KEAMANAN DIGITAL YANG WAJIB DILAKUKAN

{ Cyber.b1te }

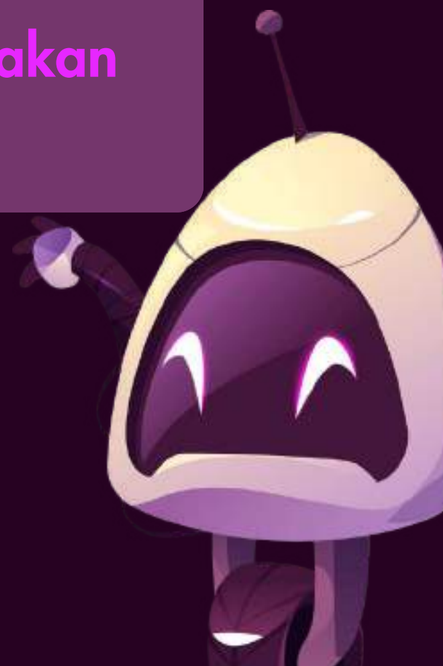
**Gunakan password manager** untuk menyimpan kata sandi dengan aman.

**Selalu update perangkat lunak dan aplikasi** untuk menutup celah keamanan.

**Hindari menggunakan Wi-Fi publik tanpa perlindungan** (gunakan VPN).

**Jangan asal mengunduh aplikasi atau klik tautan mencurigakan.**

**Laporkan aktivitas mencurigakan** untuk menutup celah keamanan.



# Keimpulan

{ Cyber.b1te }

Keamanan digital adalah tanggung jawab bersama.

Perusahaan harus menerapkan kebijakan keamanan yang ketat untuk mencegah serangan siber.

Patuhi regulasi seperti GDPR & UU ITE untuk melindungi data pribadi.

Setiap individu wajib menjaga etika digital dan tidak menyebarkan informasi palsu.

🛡️ Dengan mengikuti prinsip keamanan digital, kita dapat menjelajahi dunia maya dengan lebih aman dan nyaman!