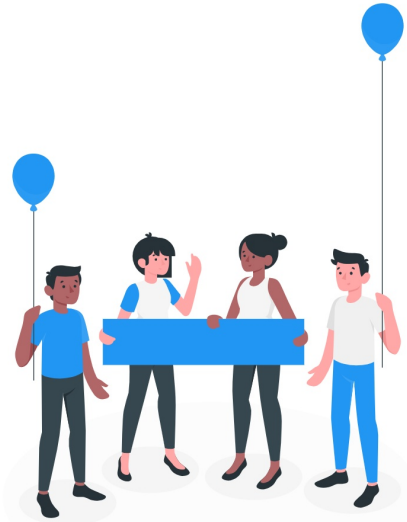

IT Awareness: Secure Your Data, Secure Your Life

Kesadaran Teknologi Informasi untuk Kehidupan yang Lebih Aman

Pendahuluan

Mengapa Keamanan Data Penting ?

01	**Kehidupan modern Bergantung pada teknologi Komunikasi, transaksi keuangan, pekerjaan, dan layanan kesehatan.**	Description of a primary heading
02	**Kebocoran data dapat menyebabkan kerugian finansial, reputasi, bahkan ancaman terhadap keselamatan pribadi.**	Description of a primary heading
03	**Evolusi Ancaman Siber Dari virus komputer sederhana hingga serangan kompleks yang melibatkan kecerdasan buatan.**	Description of a primary heading

Memahami Ancaman Dunia Digital

Phishing

Email palsu untuk mencuri data seperti username dan password.

Malware Ransomware

Memblokir akses ke data dengan tebusan.

Malware Spyware

Perangkat lunak yang mencuri atau merusak data.

Distributed Denial of Service (DDoS)

Melumpuhkan sistem dengan membanjiri lalu lintas jaringan.

Social Engineering

Manipulasi psikologi untuk mencuri data.

Mengapa Kesadaran IT Penting

Sources: Small Business Connections and Verizon, IBM Security X-Force

Statistik Global

- Jumlah serangan siber meningkat hingga 30% per tahun
- Kerugian akibat kejahatan siber diperkirakan mencapai $8 triliun pada tahun 2024
- 60% perusahaan kecil menengah gulung tikar dalam 6 bulan setelah mengalami serangan siber besar
- Kerugian global akibat serangan siber diprediksi mencapai $10 triliun pada 2025

Kerugian akibat Kebocoran Data

- Kerugian Individu
- Kerugian Organisasi

Kesadaran IT Membantu

- Mencegah serangan melalui perilaku bijak dalam menggunakan teknologi
- Melindungi data dari serangan yang tidak terlihat

Pilar Dasar Keamanan Data

Prinsip Utama Keamanan Data (CIA):

01

Confidentiality (Kerahasiaan)

Membatasi akses data hanya kepada pihak yang berwenang.

02

Integrity (Integritas)

03

Availability (Ketersediaan)

Jenis Data yang Harus Dilindungi

01 **Informasi pribadi** (KTP, nomor telepon, alamat)

02 **Data finansial** (nomor rekening, informasi kartu kredit)

03 **Data organisasi** (rahasia dagang, strategi bisnis)

Praktik Terbaik dalam Keamanan Siber

01

Lindungi Akses ke Akun Anda:

- Gunakan password yang kuat dan unik
- Terapkan autentikasi dua faktor (2FA) untuk akun sensitif

02

Jangan Abaikan Pembaruan Sistem

Pembaruan perangkat lunak memperbaiki celah keamanan

03

Gunakan Keamanan Jaringan

- Gunakan VPN saat mengakses jaringan publik
- Hindari Wi-Fi tanpa kata sandi

04

Amankan Perangkat Anda:

- Gunakan perangkat lunak antivirus
- Enkripsi data penting

05

Pahami Phishing dan Penipuan

Jangan sembarangan mengklik tautan atau mengunduh file dari sumber yang tidak dikenal

Dampak Kebocoran Data bagi Individu

Kebocoran data dapat menyebabkan kerugian yang signifikan bagi individu.

01

Pencurian Identitas

Informasi pribadi yang bocor dapat digunakan untuk pencurian identitas.

02

Kerugian Finansial

Informasi pembayaran yang bocor dapat digunakan untuk transaksi tidak sah.

03

Risiko Terhadap Privasi

Data pribadi yang bocor dapat menyebabkan reputasi rusak.

04

Gangguan Psikologis

Individu dapat merasa cemas dan kehilangan kepercayaan.

05

Kerugian dalam Kredibilitas Online

Individu dapat kehilangan kontrol atas citra online mereka.

Keamanan di Media Sosial dan Aplikasi

Kebocoran data dapat menyebabkan kerugian yang signifikan bagi individu.

01

Periksa Pengaturan Privasi

Setel privasi akun sosial media untuk membatasi siapa yang bisa melihat informasi pribadi

02

Waspada terhadap Aplikasi Pihak Ketiga

- Aplikasi atau game yang meminta akses ke informasi pribadi tanpa alasan jelas harus dihindari
- Tinjau dan batalkan aplikasi yang tidak lagi digunakan

03

Mencegah Pencurian Identitas

- Hindari membagikan informasi sensitif secara terbuka di platform media sosial
- Tidak sembarang login di berbagai device dan pastikan logout/lockscreen Ketika meninggalkan device
- Gunakan fitur verifikasi dua langkah untuk akun penting

Pengelolaan Risiko IT dalam Organisasi

Kebijakan IT yang Kuat

Implementasi aturan ketat tentang akses data dan perangkat

Pendidikan dan Pelatihan

Latih karyawan untuk mengenali ancaman siber

Rencana Pemulihan

Siapkan disaster recovery plan untuk menghadapi insiden keamanan

Audit Keamanan Berkala

Lakukan penilaian rutin terhadap sistem dan data.

Dampak Kebocoran Data bagi Organisasi

Kerugian Finansial Langsung 01

- Denda dan Ganti Rugi
- Biaya Pemulihan
- Kerugian dalam Penanganan Kasus Hukum

Reputasi Rusak 02

- Kehilangan Kepercayaan Pelanggan
- Kehilangan Pangsa Pasar
- Pengaruh Jangka Panjang pada Merek

Gangguan Operasional 03

- Waktu Henti Sistem (Downtime)
- Biaya Pemulihan Infrastruktur IT

Risiko terhadap Inovasi dan Pengembangan Produk 04

Mengalihkan fokus ke masalah keamanan dan pemulihan, bukan pada inovasi

Keamanan dan Regulasi yang Lebih Ketat 05

- Menghadapi pemeriksaan lebih ketat dari regulator
- Mengeluarkan biaya lebih dalam investasi keamanan IT

Pengaruh pada Hubungan dengan Mitra Bisnis 06

- Kehilangan kepercayaan
- Mungkin kesulitan untuk menarik mitra atau investor baru

Contoh kasus nyata

Disclaimer : data berikut bukan bermaksud menggiring opini pada kredibilitasnya, tetapi untuk pelajaran sesuai sumber terpublikasi

Kebocoran Data di Tokopedia (2020)

Kasus: Pada Mei 2020, Tokopedia, salah satu perusahaan e-commerce terbesar di Indonesia, mengalami kebocoran data yang sangat besar. Data lebih dari 91 juta akun pengguna bocor, yang melibatkan informasi seperti nama, email, alamat, nomor telepon, serta beberapa data lain yang dapat diakses oleh pihak yang tidak bertanggung jawab.

Kebocoran data di Pusat Data Nasional PDN (2023)

Pada Juni 2023, PDN Sementara 2 di Surabaya mengalami serangan ransomware oleh kelompok hacker bernama Brain Cipher Ransomware. Hacker ini mengenkripsi ribuan terabyte data dari sistem PDN dan meminta tebusan sebesar $8 juta (sekitar Rp131 miliar). Pemerintah Indonesia menolak membayar tebusan tersebut. Sebagai respons, kelompok tersebut memberikan kunci dekripsi secara gratis, tetapi mereka menuntut pengakuan dari pemerintah atas bantuan tersebut

Kesimpulan

1. Kesadaran IT adalah langkah awal melindungi data dan masa depan.
   Description of a primary heading

2. Individu dan organisasi harus bekerja sama menghadapi ancaman digital
   Description of a primary heading

3. **Keamanan IT adalah Tanggung Jawab Bersama: Keamanan data bukan hanya tanggung jawab tim IT, tetapi seluruh individu yang menggunakan teknologi.**
   Description of a primary heading

4. **Kesadaran akan ancaman dan penerapan praktik terbaik dapat melindungi individu, organisasi, dan masyarakat secara keseluruhan.**
   Description of a primary heading

Thankyou