Pertemuan 4

OuTLine

1. Studi kasus kebocoran data
2. Mengelola Identitas Digital
3. Penanggulangan kebocoran data
4. Praktik pengelolaan password di internet

Kebocoran Data / Data Leakage

Kebocoran data adalah suatu kondisi dimana data sensitif secara tidak sengaja terekspose atau terakses oleh pihak tidak sah. Ancaman ini dapat terjadi melalui situs website, email, hard drive, atau pun laptop.

Kebocoran data (data leakage) memiliki arti yang berbeda dengan pelanggaran data (data breach). Berikut perbedaan keduanya :

- Data breach adalah serangan yang sengaja dilakukan untuk membobol sistem sehingga data sensitif dapat diakses.
- Data leakage tidak memerlukan serangan cyber khusus karena pada umumnya kebocoran data dapat terjadi karena data security yang buruk atau karena kelalaian pengguna sendiri.

Penyebab Kebocoran Data

1 *Human Error* baik yang disengaja atau tidak

Sebagian besar, insiden kebocoran data karena *human error*. Contohnya, kasus ini bisa terjadi ketika programmer membuat *database* yang tersedia untuk umum dan mesin pencari, yakni kondisi saat informasi rahasia perusahaan bocor dan siapa pun dapat memperoleh akses tersebut sampai terkunci kembali. Ketika kesalahan ini terjadi, mereka yang ingin meretas sistem perusahaan akan mencetak informasi rahasia sehingga mereka dapat menggunakannya di masa depan.

Meski begitu, semua kebocoran data yang tidak disengaja tetap mengakibatkan hukuman dan kerusakan reputasi yang sama.

2 Malicious Software (Malware)

Malware adalah program yang dirancang untuk merusak dengan menyusup ke sistem komputer. Penyusupan tersebut bisa masuk melalui *email*, *download* internet, atau program yang terinfeksi.

Malware juga dapat menyebabkan kerusakan pada sistem komputer dan memungkinkan terjadinya pencurian informasi perusahaan. Maka dari itu, Anda perlu berhati-hati dalam mengakses *website* yang terlihat mencurigakan atau membuka email dari pengirim yang tidak dikenal. Keduanya menjadi metode populer untuk menyebarkan *malware*, sehingga *data security* menjadi lemah dan berpotensi bocor.

Dampak Kebocoran Data

1 *Legal Liability*

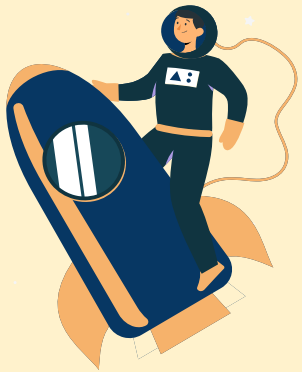
Perusahaan yang lengah dalam melindungi data penting miliknya, terutama yang mengandung informasi pelanggan, akan berhadapan dengan UU ITE 2008.

2 *Lost Productivity*

Dapat mengakibatkan lost productivity bagi perusahaan yang tidak teliti dalam menjaga hasil penemuan, desain baru, ide pemasaran, dan sebagainya karena sudah bocor dan berpotensi pindah ke perusahaan lain.

3 *Business Reputation*

Perusahaan yang lengah dalam melindungi data penting miliknya, terutama yang mengandung informasi pelanggan, akan berhadapan dengan UU ITE 2008.



Menghindari Kebocoran Data

1 Perusahaan harus membuat kebijakan keamanan

Perusahaan harus mulai mengembangkan seperangkat pedoman yang harus diikuti karyawannya. Contohnya adalah seperti menegakkan peraturan bahwa karyawan tidak boleh meninggalkan komputer dalam keadaan logged on/unlocked, tidak berbagi akun dengan rekan kerja yang lain, dan lain-lain.

2 Mengontrol konten dalam email

Untuk meminimalisir hal kebocoran data melalui email, perusahaan Anda dapat menggunakan email content filtering. Email filter akan melakukan proses penyaringan lalu lintas email baik itu pesan masuk atau pesan keluar. Filter akan memindai pesan dan mengklasifikasikan pesan ke dalam kategori yang berbeda seperti spam, virus, penipuan, dan lain-lain.

3 Endpoint Protection

Email filter akan melakukan proses penyaringan lalu lintas email baik itu pesan masuk atau pesan keluar. Filter akan memindai pesan dan mengklasifikasikan pesan ke dalam kategori yang berbeda seperti spam, virus, penipuan, dan lain-lain. Teknologi ini juga dapat memperingatkan administrator tentang ancaman orang dalam. Sistem akan memberi tahu jika terdapat pengguna yang mencoba mengirim info sensitif ke luar perusahaan.

4 Meningkatkan keamanan data

Salah satu cara untuk menghindari bocornya data adalah dengan selalu memastikan bahwa sistem yang digunakan memiliki keamanan yang baik. Caranya adalah dengan melakukan penetration testing secara rutin. Dengan penetration testing, kerentanan keamanan dapat segera ditemukan dan diperbaiki sehingga data dapat terlindungi.

Kebocoran Data

Kebocoran Data Tokopedia

Jakarta, CNN Indonesia -- Tokopedia dilaporkan mengalami peretasan, bahkan jumlahnya diperkirakan 91 juta akun dan 7 juta akun merchant, tidak lagi 15 juta seperti diberitakan sebelumnya. Padahal di tahun 2019, Tokopedia mengungkapkan bahwa ada sekitar 91 juta akun aktif di platformnya.

Artinya hampir semua akun di Tokopedia berhasil diambil datanya oleh peretas. Pelaku menjual data di *darkweb* berupa user ID, email, nama lengkap, tanggal lahir, jenis kelamin, nomor handphone dan password yang masih ter-hash atau tersandi.

Semua dijual dengan harga US$5.000 atau sekitar Rp74 juta. Bahkan ada 14.999.896 akun Tokopedia yang datanya saat ini bisa didownload.

Adapun kronologi lengkap bobolnya akun Tokopedia tersebut bermula saat peretas Whysodank pertama kali mempublikasikan hasil peretasan di Raid Forum pada Sabtu (2/5). Peretasan tersebut terjadi pada 20 Maret 2020.

Kemudian, akun @underthebreach sore harinya pukul 16:15 WIB mencuitkan soal peretasan dan mengaku sebagai layanan pengawasan dan pencegahan kebocoran data asal Israel. Cuitan ini disampaikan sembari menyolek akun resmi Tokopedia.

Dalam tangkapan layar yang dibagikan di media sosial disebut kalau peretas masih harus memecahkan algoritma untuk membuka hash dari password para pengguna itu. Peretas pun meminta bantuan peretas lain untuk membuka kunci algoritma itu.

https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual

Kebocoran Data

Kebocoran Data BPJS Kesehatan

Bareskrim Geledah Kantor BPJS Kesehatan soal Kebocoran Data

CNN Indonesia | Jumat, 25/06/2021 15:01 WIB

Bagikan :

https://www.cnnindonesia.com/nasional/20210625142716-20-659389/bareskrim-geledah-kantor-bpjs-kesehatan-soal-kebocoran-data

Jakarta, CNN Indonesia -- Badan Reserse Kriminal (Bareskrim) Polri menggeledah kantor BPJS Kesehatan yang terletak di wilayah DKI Jakarta selama tiga hari berturut-turut.

Penggeledahan dilakukan terkait proses penyelidikan dugaan kebocoran data yang menyebabkan data kependudukan masyarakat tersebar dan dijual di forum daring beberapa waktu lalu.

Baca juga: Ahli Sebut Kerugian Kebocoran Data Penduduk-BPJS Rp600 T

"Telah dilakukan penggeledahan pada tanggal 8,9 dan 10 Juni 2021 di kantor BPJS Kesehatan terhadap server BPJS Kesehatan di Jakarta Pusat," kata Kepala Bagian Penerangan Umum (Kabagpenum) Polri Kombes Ahmad Ramadhan kepada wartawan, Jumat (25/6).

Ramadhan mengungkapkan bahwa pihak penyidik turut menyita dua laptop di dalam kantor tersebut. Kata dia, saat ini tim forensik tengah melakukan pendalaman terhadap laptop tersebut.

Kemudian, kata dia, penyidik juga telah menerima data dari PT S terkait dengan hasil Penetration Testing (Pentest) atau pengujian keamanan informasi.

Diketahui, upaya Pentes tersebut dilakukan dengan simulasi seorang asesor meniru serangan yang biasa sering terjadi untuk mengidentifikasi metode peretasan fitur keamanan aplikasi, sistem, atau jaringan.

"Pada tanggal 10 Juni 2021, Tim Forensik Siber Bareskrim telah melihat secara langsung database BPJS Kesehatan," ucapnya.

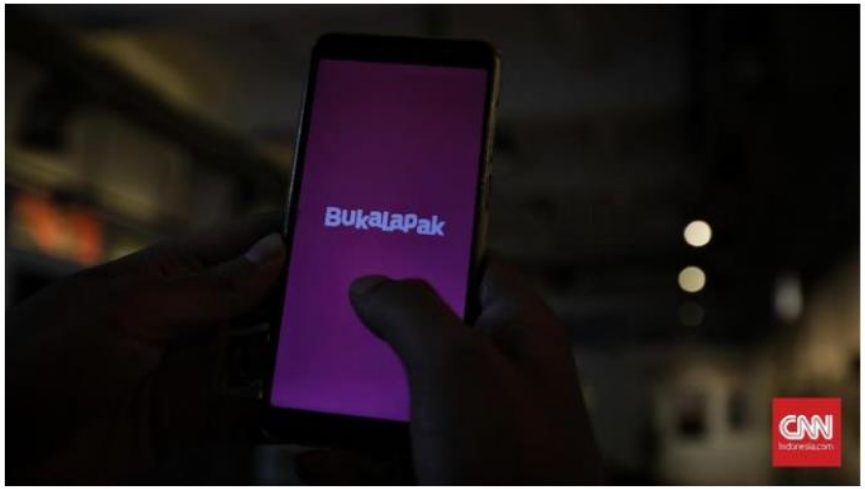
Kebocoran Data

Kebocoran Data Bukalapak

13 Juta Data Bocor Bukalapak Dijual di Forum Hacker

eks, CNN Indonesia | Rabu, 06/05/2020 06:59 WIB

Bagikan :



Jakarta, CNN Indonesia -- Data 13 juta akun Bukalapak yang bocor kembali diperjualbelikan di forum *hacker* RaidForums. Data ini dijual oleh dua akun penjual di forum yang sebelumnya menjadi tempat penjualan 91 juta pengguna Tokopedia.

Berdasarkan pantauan CNNIndonesia.com, Rabu (6/5), penjual dengan nama akun Asian Boy menyebut data yang ia jual tertanggal tahun 2017.

"Saya menjual basis data Bukalapak.com, 12.960.526 pengguna," tulis Asian Boy dalam *thread* di forum itu.

Data yang ditampilkan mulai dari email, nama pengguna, *password*, *salt*, last login, *email* Facebook dengan *hash*, alamat pengguna, tanggal ulang tahun, hingga nomor telepon. Ia mengeposkan jualan ini sekitar pukul 01.00 WIB.

Penjual pertama ini baru bergabung di forum tersebut bulan April 2020 dan baru mengeposkan 3 *thread*. Ketiga *thread* tersebut berupa jualan data dari beberapa situs lain yaitu Classpass dan Reverbnation. Pengguna ini belum memiliki reputasi.

Sementara penjual yang lain dengan nama akun Tryhard User juga menawarkan 12 juta data Bukalapak. Dalam contoh data yang ia tampilkan, tampak beberapa data pendiri Bukalapak seperti Fajrin Rasyid hingga Ahmad Zaky.

"Menjual basis data Bukalapak.com," tulisnya.

Tryhard User sudah lebih lama menjadi penghuni Raid Forums. Dalam biografi tercatat ia sudah bergabung sejak April 2017. Nilai reputasi pun cukup tinggi 546 dengan 48 thread. Ia mengeposkan jualan data itu pada Senin (4/5) pukul 20:58.

Keduanya tidak mencantumkan berapa data itu mereka jual, sebab mereka meminta untuk mengontak langsung untuk menanyakan harga.

CNNIndonesia.com telah mengontak Bukalapak untuk mengonfirmasi hal ini namun belum mendapat respons.

https://www.cnnindonesia.com/teknologi/20200506065657-185-500477/13-juta-data-bocor-bukalapak-dijual-di-forum-hacker

Identitas Digital

Dalam sebuah sistem identitas digital, identitas merupakan kumpulan dari catatan digital yang mewakili seorang warga. Seluruh catatan ini disimpan oleh sebuah institusi yang memang menyediakan identitas digital ini.

Sistem identitas digital ini bisa mempermudah proses dokumentasi warga negara dan mengumpulkan data-data yang penting milik mereka. Berkat sistem autentikasi dan keamanan yang canggih, sistem identitas digital tidak akan bisa dipalsukan, dicuri, ataupun hilang dibandingkan dengan identitas manual. Sehingga kita tidak perlu khawatir lagi dalam urusan membawa dan menyimpan identitas kita.

https://blog.privy.id/7-kegunaan-sistem-identitas-digital/

Manfaat Identitas Digital

1

Dilindungi oleh sistem keamanan yang paling canggih

Identitas digital warga disimpan pada server terpercaya, dilengkapi dengan sistem yang canggih. Pengguna bisa mengetahui siapa saja yang dapat melihat identitas digital. Bila ada kegiatan seperti pencurian data identitas atau pemalsuan maka bisa diketahui dengan cepat.

2

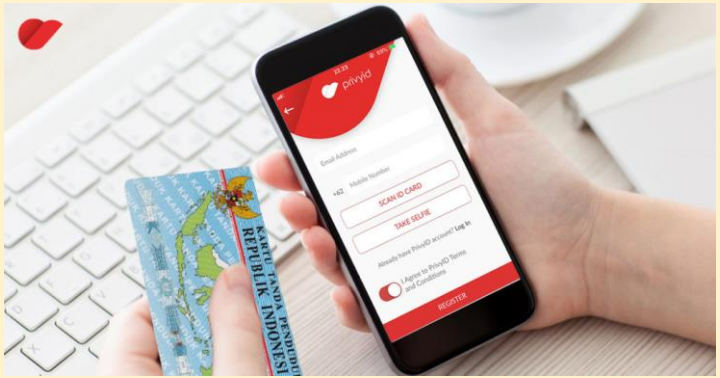
Privasi identitas terjaga

Anda pasti berpikir bahwa identitas digital bisa diakses oleh siapa saja namun, Anda salah karena identitas digital hanya dapat dilihat oleh orang tertentu sesuai dengan pilihan. Terdapat pengaturan khusus untuk menentukan siapa saja yang boleh mengakses informasi identitas digital Anda.

3

Lebih Praktis

Seperti yang telah Kita ketahui bahwa identitas digital tersimpan pada satu server. Pengecekan identitas bisa dilakukan secara langsung pada internet tanpa harus mengeluarkan lembaran kertas. Oleh sebab itu identitas digital ini dinyatakan lebih praktis. Bahkan ketika melakukan transaksi belanja, Anda tidak perlu mengisi formulir. Cukup menunjukkan identitas digital saja, belanja bisa diproses dengan cepat.



https://idcloudhost.com/manfaat-dan-prinsip-mengolah-identitas-digital/

Manfaat Identitas Digital

4

Transparan

Manfaat mengolah identitas digital selanjutnya yaitu pengguna dapat mengetahui adanya perubahan data. Jika ada oknum yang tidak bertanggung jawab ingin mengubahnya maka, Anda bisa mencegahnya.

5

Membangun ekonomi digital

Pembangunan ekonomi digital mulai dilakukan oleh Negara. Dengan adanya identitas digital akan terbangun jaringan yang kuat, jaringan tersebut dilakukan antara pembuat identitas digital, pengguna identitas serta pihak lainnya. Hal ini dapat membantu perekonomian digital makin berkembang, sampai akhirnya memudahkan transaksi elektronik pada masa depan

https://idcloudhost.com/manfaat-dan-prinsip-mengolah-identitas-digital/

Mengamankan Identitas Digital

1 Gunakan Identitas Digital Lebih dari Satu

Langkah awal yang bisa kita lakukan adalah jangan buat satu identitas digital saja. Dengan identitas digital yang berbeda-beda ini, maka kita pun akan lebih mudah melakukan pengelolaan, sekaligus melindungi data penting. Misalnya saja sebagai berikut:

- **Identitas digital primer** yang hanya bisa Anda gunakan untuk keperluan penting. Seperti keperluan yang menyangkut lembaga negara, keuangan, dan perbankan. Jangan menyebarkan link yang berhubungan dengan lembaga tersebut ke media sosial, termasuk menyebarkan email dari lembaga terpercaya tersebut bila memang tidak penting.
- **Identitas digital sekunder**. Identitas digital ini bisa Anda gunakan untuk keperluan tertentu saja. Misalnya untuk layanan internet, telepon seluler, TV kabel, dan sebagainya dan terpisah dari identitas primer.
- Berikutnya adalah **identitas digital untuk media sosial**. Untuk ini, Anda dapat menggunakan identitas digital tersebut seperti email hanya untuk membuat atau mendaftar ke media sosial.

Mengamankan Identitas Digital

2 Berikan Data kepada Pihak yang Tepat

- ✓ Jika memang Anda harus menyerahkan data pribadi maka pastikan data Anda diberikan kepada lembaga terpercaya dan untuk konteks yang penting. Misalnya untuk pendataan penduduk, sensus, dan sebagainya yang diselenggarakan oleh negara.

- ✓ Selain itu Anda juga harus memahami izin ataupun sertifikasi penyimpanan data identitas yang dilakukan perusahaan terkait. Hal ini dimaksudkan agar data tidak hanya berada di tangan yang tepat, tetapi juga disimpan dengan protokol keamanan yang kuat.

Mengamankan Identitas Digital

3

Gunakan Tanda Tangan Digital yang Terverifikasi

Tanda tangan digital dalam mengamankan identitas digital pada dasarnya dibagi menjadi dua jenis yakni *basic* dan *advanced and qualified*.

Basic. Menggunakan metode kriptografi asimetris. Metode ini memiliki kelemahan yaitu tidak melalui proses otentikasi dua langkah. Sehingga dari segi kekuatan hukumnya lemah meskipun memiliki enkripsi.

A*dvanced and qualified*. Memiliki kekuatan hukum yang kuat dan kedudukannya setara dengan tanda tangan basah pada kertas. Dilengkapi dengan kriptografi asimetris dan *public key infrastructure*. Penyedia layanan tanda tangan *advanced and qualified* pun diharuskan sudah menerapkan kebijakan proses otentikasi dua langkah.

Salah satu penyedia layanan tanda tangan digital jenis *advanced and qualified* yang ada di Indonesia adalah Vida.id. Vida.id memiliki fitur otentikasi pemindaian wajah dengan UI Wireframe yang terstandardisasi.

Biometrik/Sidik Jari

Pin dan Password

https://money.kompas.com/read/2021/07/24/195414126/mengenal-kode-otp-dan-bedanya-dengan-pin

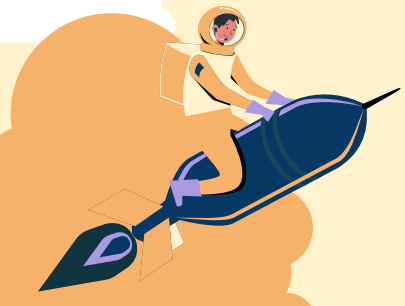
OTP adalah kode password yang bersifat sementara yang dikirimkan melalui pesan singkat.

Kode OTP adalah sarana keamanan yang dibuat pembuat aplikasi agar tidak disalahgunakan orang lain. Ini karena penerima kode OTP adalah pemilik nomor handpone atau email yang didaftarkan.

Di era digitalisasi saat ini, kode OTP dipakai untuk pembuat aplikasi untuk proses pendaftaran. Seperti pendaftaran rekening bank digital, pendaftaran akun e-commerce, pendaftaran akun dompet digital, dan aplikasi lainnya.

e-KYC (Electronic Know Your Customer)

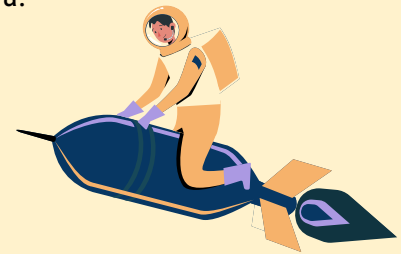
eKYC adalah prosedur untuk mengidentifikasi dan melakukan verifikasi identitas pelanggan secara digital atau online. Proses dari eKYC terdiri dari serangkaian pemeriksaan yang dilakukan pada tahap pertama komunikasi dengan klien untuk verifikasi bahwa mereka adalah orang yang sesuai dengan identitas



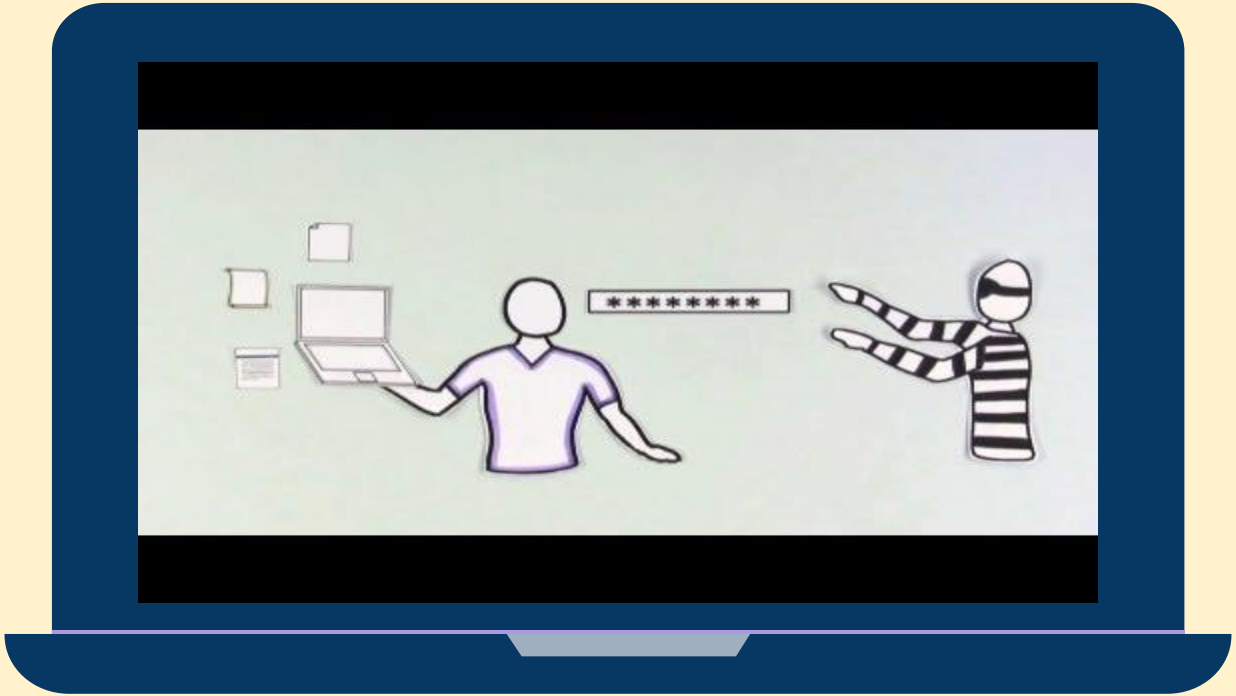
e-KYC (Electronic Know Your Customer)

Digital signature merupakan tanda tangan yang terdiri atas informasi elektronik yang dilekatkan, terasosiasi atau terkait dengan informasi elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi.

Fitur sekuriti ini dapat dimanfaatkan sebagai sebuah bukti dari adanya identitas suatu pihak yang dapat menunjukkan subjek hukum pihak tersebut. Digital signature diimplementasikan pada sertifikat elektronik sehingga dokumen elektronik yang ditransaksikan dapat diketahui keabsahan dan keasliannya.

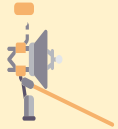


Mengelola Password



https://youtu.be/aEmF3Iylvr4

Tips Membuat Password yang Kuat



Jangan pernah menggunakan informasi pribadi Anda seperti nama, ulang tahun, username, atau alamat email.

Gunakan password yang panjang. Setidaknya panjang password minimal 8 digit, meskipun dapat lebih panjang untuk keamanan ekstra.

Jangan memakai password yang sama untuk semua akun Anda. Jika seseorang menemukan kata sandi pada satu akun Anda, maka akun-akun Anda lainnya akan terancam.

Gunakan kombinasi angka, simbol, huruf kapital dan kecil. Contoh : uN5S0!o, 19PasW0rD4kOe

Hindari menggunakan kata-kata yang dapat ditemukan di dalam kamus. Misalnya, berenang1 merupakan password yang lemah.

Password acak adalah password yang terkuat. Jika Anda mengalami kesulitan membuat password acak ini, maka Anda dapat menggunakan aplikasi password generator.

https://edu.gcfglobal.org/en/tr_id-internet-safety/membuat-kata-sandi-password-yang-kuat/1/

2 Step Verification

Protect your account with 2-Step Verification

With 2-Step Verification (also known as two-factor authentication), you add an extra layer of security to your account in case your password is stolen. After you set up 2-Step Verification, you'll sign in to your account in two steps using:

- Something you know, like your password
- Something you have, like your phone

Turn on 2-Step Verification

1. Open your Google Account.
2. In the navigation panel, select **Security**.
3. Under "Signing in to Google," select **2-Step Verification** > **Get started**.
4. Follow the on-screen steps.

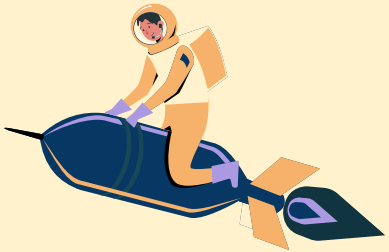
Your account, username@gmail.com, is associated with your work or school. If you can't set up 2-Step Verification, contact your administrator.

Verify it's you with a second step

After you turn on 2-Step Verification, you'll need to complete a second step to verify it's you when you sign in. To help protect your account, Google will request that you complete a specific second step.

Two Factor Authentication atau biasa disebut 2FA adalah salah satu peningkatan standar keamanan yang membutuhkan 2 proses identifikasi.

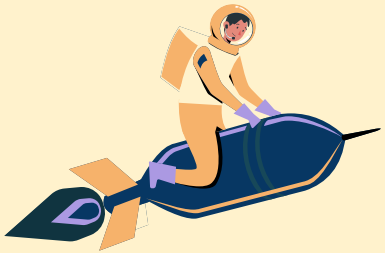
Yaitu menggunakan password dan security code (kode keamanan)

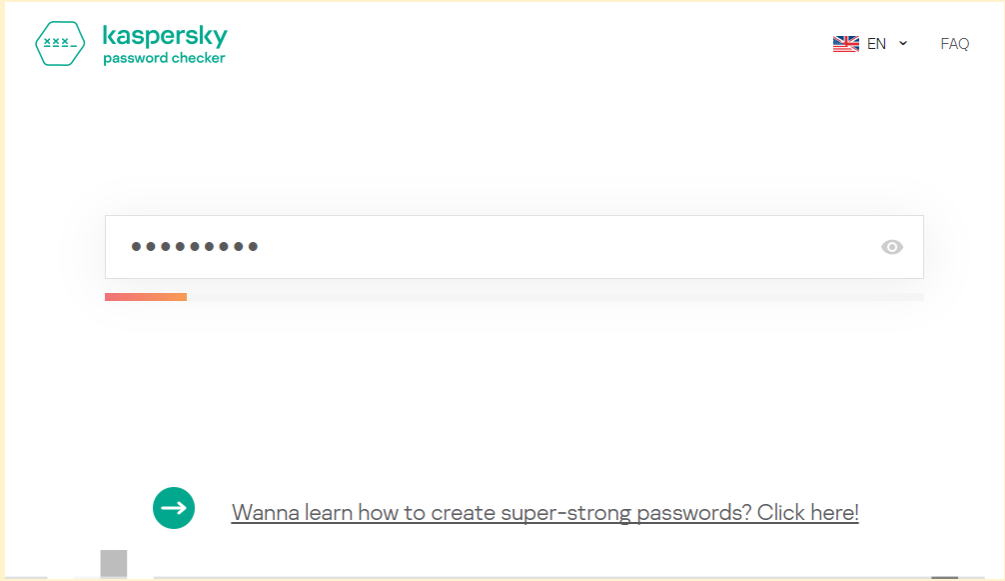


Password Tester

Sebelum kita menggunakan password yang kita buat, alangkah baiknya jika kita melakukan testing terlebih dahulu. Tujuannya adalah untuk mengetahui apakah password yang kita pakai aman atau tidak.

Kaspersky menyediakan sebuah aplikasi yang dapat kita gunakan untuk mengecek tingkat keamanan password yang kita buat.





https://password.kaspersky.com/

Tugas 3

Membuat artikel terkait kebocoran data, identitas digital, dan keamanan digital. Poin-poin yang dibahas adalah

1. Pilih salah satu topik (berita) yang memuat tentang kebocoran data. Boleh bersumber dari dalam atau luar negeri
2. Bagaimana kebocoran data itu bisa terjadi ? Tuliskan analisis kalian masing-masing !
3. Bagaimana sikap anda menyikapi hal tersebut ? Apa yang anda lakukan untuk menghindari hal tersebut ? Jelaskan alasan anda !
4. Jika anda adalah seorang pekerja seni/ penyedia konten kreatif. Langkah apa yang anda lakukan untuk mengamankan dan melindungi produk/karya anda ?

Tugas ditulis di Ms. Word

Pengumpulan tugas paling lambat tanggal 22 September jam 23.59 di SPADA