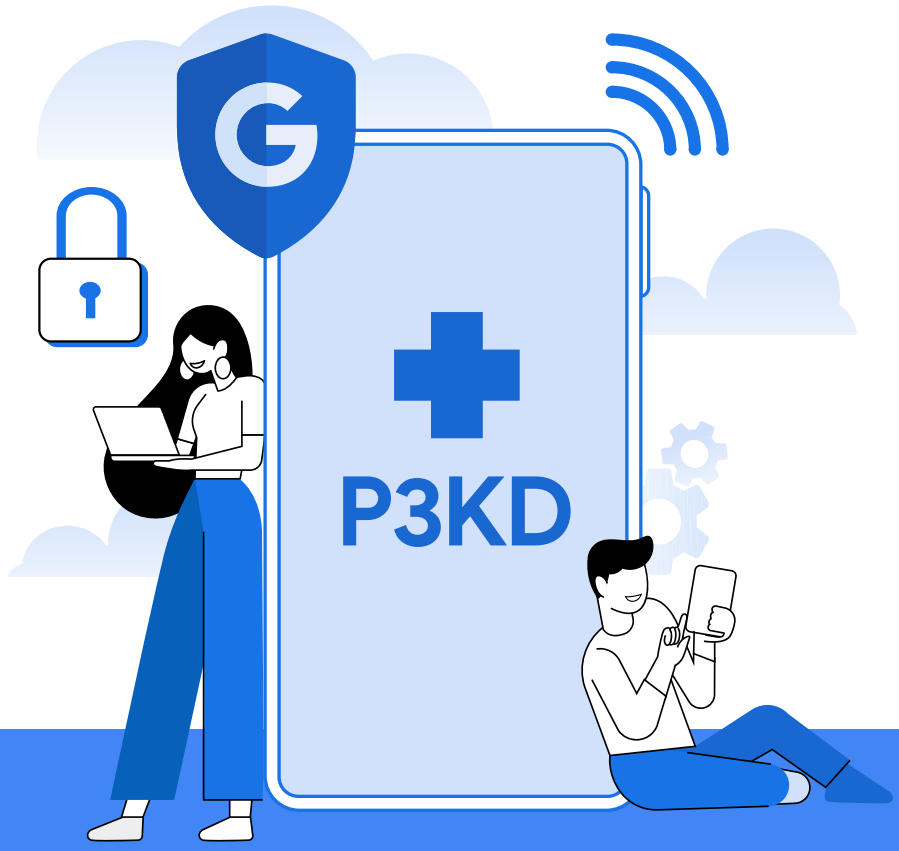
Tips Keamanan Berinternet



P3KD

Safer with Google

Perlindungan Pertama
Perkuat Keamanan Digital

KOMINFO SIBER KREASI ICT Watch! Indonesia Masyarakat Anti Fitnah Indonesia Turn Back Hoax Mafindo Google

Daftar isi

Klik teks untuk mengunjungi halaman spesifik

Tips Keamanan Siber

Tips Privasi Data

Tips Keamanan Siber

P3KD

Safer with Google

Beri perlindungan kuat untuk akun & perangkatmu

Membuat sandi yang kuat dan unik untuk setiap akun merupakan salah satu langkah terpenting dalam melindungi privasimu.

Buat sandi yang kuat & unik

Tips #1

Sandi harus terdiri dari minimal 8 karakter.

Tips #2

Gunakan kombinasi huruf besar, huruf kecil, angka, dan simbol.

Tips #3

Jangan gunakan informasi pribadi dalam sandimu, seperti: nama, alamat, email, nomor ponsel, nomor KTP, nama ibu/ayah, hari ulang tahun atau nama binatang peliharaan, dll.

Tips #4

Jangan gunakan sandi yang mudah ditebak, misalnya nomor berurutan, seperti "123456" atau "password123"!

Beri perlindungan kuat untuk akun & perangkatmu

Menjaga keamanan sandi sama pentingnya dengan membuat sandi yang kuat.
Ikuti tips praktis ini untuk melindungi sandi dengan mudah!

Jaga sandimu tetap aman

Tips #1

Jangan pernah menyimpan sandi di tempat yang bisa ditemukan orang lain atau membagikan sandimu dengan siapa pun.

Tips #2

Gunakan sandi yang berbeda untuk setiap akunmu.

Tips #3

Gunakan Pengelola Sandi Google untuk membantumu membuat, menyimpan, dan mengelola sandimu, serta memperingatimu bila ada sandi yang disusupi.

Tips #4

Seperti halnya kesehatan yang perlu check-up berkala, begitu juga dengan sandimu! Gunakan Pemeriksaan Sandi Google untuk mendeteksi jika ada sandimu yang telah disusupi, sandi yang lemah (baik di akunmu mau pun di situs pihak ketiga), serta mengubah sandimu dengan mudah.

Cool tips!

Buat sandi yang sulit ditebak, tapi gampang diingat dengan membuat kalimat acak!

Contoh kalimat:

Aku suka makan nasi goreng dan naik dinosaurus.

Contoh password:

Ambil huruf pertama dari setiap kata dalam kalimat.
Contoh: **asmngdnd**

Tambahkan huruf besar & huruf kecil: **asmNGdnD**
→ Supaya gampang diingat, huruf besar diletakkan pada inisial "**n**asi **g**oreng" dan "**d**inosaurus".

Terakhir, tambahkan angka & simbol: **45mNG&nD**
→ Ubah beberapa huruf dengan angka, ganti kata "dan" dengan simbol "&".

Kamu bisa menerapkan formula yang sama setiap membuat sandi untuk akun baru.
Contoh: Aku suka makan **m**ie **a**yam dan naik **k**uda!
→ **45mMA&nK!**

Beri perlindungan kuat untuk akun & perangkatmu

Salah satu cara terbaik untuk melindungi akunmu dari upaya pembobolan, yaitu dengan mengaktifkan Verifikasi 2 Langkah.

Gunakan Verifikasi 2 Langkah

Contoh penerapan Verifikasi 2 Langkah

Saat kamu mencoba login ke akun bankmu, selain sandi/pin, biasanya kamu akan diminta memasukkan kode verifikasi yang dikirimkan via SMS ke nomor ponselmu.

Tips #1

Aktifkan Verifikasi 2 Langkah di menu Pengaturan akunmu. Khusus untuk Akun Google, akses menu Keamanan di sini & cek panduannya di sini.

Tips #2

Saat mengaktifkan Verifikasi 2 Langkah, pastikan kamu **menghubungkannya dengan nomor ponsel dan perangkat yang paling sering kamu gunakan**, karena fitur ini akan mengirimkan notifikasi ke perangkat tersebut untuk menyelesaikan login.

Tips #3

Jika kamu kehilangan perangkat atau mengganti nomor ponselmu, lalu tidak bisa login dengan Verifikasi 2 Langkah, klik di sini dan ikuti langkah untuk memulihkan akunmu.

Safer with Google

Cool tips!

Jika kamu sudah memahami konsep **Verifikasi 2 Langkah**, kamu juga bisa coba menggunakan aplikasi Google Authenticator untuk pengiriman kode keamanan.

Aplikasi ini **gratis** dan memungkinkan kamu untuk menerima kode bagi **beberapa akun sekaligus, tanpa internet atau pun layanan seluler**.

Download sekarang di
Google Play Store atau Apple App Store.

Tahukah kamu?

Sejak tahun 2021, Google telah berhasil menerapkan pengaktifan fitur Verifikasi 2 Langkah **secara otomatis untuk 150 juta pengguna di seluruh dunia.** Hasilnya, pembobolan akun para pengguna tersebut menurun **hingga 50%.**

Beri perlindungan kuat untuk akun & perangkatmu

Melindungi akunmu dari upaya kejahatan dimulai dari dasar, seperti halnya pagar yang melindungi rumah. Ikuti tips ini untuk belajar melindungi keamanan dirimu di internet!

Menjaga keamanan perangkat

Tips #1: Jangan abaikan notifikasi software update!

Update software dan aplikasi yang kamu gunakan secara berkala, serta pastikan perangkatmu menggunakan update terbaru yang tersedia.

Tips #2: Lindungi keamanan datamu dari aplikasi berbahaya

- Pastikan kamu selalu download aplikasi dari sumber resmi dan tepercaya, seperti Google Play.
- Hapus aplikasi yang sudah tidak digunakan.
- Aktifkan update otomatis pada aplikasi.
- Batasi akses aplikasi ke data sensitif, seperti lokasi dan foto.

Tips #3: Gunakan kunci layar

Saat tidak menggunakan komputer, laptop, tablet, atau ponsel, kunci layar agar orang lain tidak dapat login ke perangkatmu. Untuk keamanan tambahan, atur perangkatmu agar mengunci layar secara otomatis saat perangkat beralih ke mode tidur.

Tahukah kamu?

Google Play Protect melakukan
pemindaian keamanan pada **125 miliar aplikasi**
terinstal setiap hari.

Sumber: Data Internal Google, 2022

Menjelajahi internet dengan aman

Di internet ada situs-situs tidak aman yang dapat mencuri informasi yang kamu masukkan. Pelajari cara memastikan keamanan situs dan jaringan yang kamu gunakan dengan mengikuti tips berikut.

Pastikan URL situs web aman

Tips #1: Cek ikon gembok terkunci dan "https" pada URL

Hindari memasukkan informasi sensitif, seperti sandi atau nomor kartu kredit sebelum memastikan situs tersebut aman.

Cek URL situsnya. Pada browser Google Chrome, jika situs tersebut aman, di kolom URL akan muncul ikon gembok terkunci dan diawali dengan "http**s**" (perhatikan adanya huruf "**s**" = "**secure**").

Pastikan koneksimu aman

Tips #2: Berhati-hati saat menggunakan Wi-Fi publik

Jaringan Wi-Fi publik atau gratis, mungkin tidak dienkripsi—sekalipun dibutuhkan sandi untuk mengaksesnya, sehingga saat terhubung ke jaringan tersebut, siapa pun yang berada di sekitar jaringan dapat memantau aktivitas internetmu.

Tonton video ini untuk tips mengamankan jaringan Wi-Fi milikmu.

Phishing

Phishing merupakan tindak kejahatan siber, di mana pelaku memperdayai dan membujuk korban via email, media sosial, dll. untuk membagikan data sensitif, seperti informasi login, bank, kartu kredit, dll.

Guna menghindari phishing, tanyakan pertanyaan berikut sebelum kamu mengklik link atau merespon pesan

Pertanyaan #1: Sebelum mengklik suatu URL (link), cari tahu sendiri secara online **nama dan URL resmi bisnisnya**. Bandingkan, apakah sesuai dengan yang kamu terima? Hal ini karena penipu kadang membuat URL dan halaman situs web yang mirip dengan perusahaan resminya untuk menipumu.

Pertanyaan #2: Cek apakah tampilan pesan atau situs terlihat **profesional**, dengan produk atau logo perusahaan yang **benar, tanpa kesalahan ejaan?**

Pertanyaan #3: **Apakah ada peringatan?** Gmail menandai email mencurigakan dan memindai lampiran bervirus secara otomatis. Perhatikan peringatan yang diberikan sistem seperti "tandai sebagai spam" atau "virus terdeteksi".

Pertanyaan #4: Apakah pesan atau hal yang ditawarkan **terdengar mustahil?** Misalnya, kesempatan untuk menghasilkan uang yang sangat banyak atau memenangkan sesuatu. Kemungkinan besar ini adalah upaya penipuan.

Pertanyaan #5: Apakah pesannya **terdengar aneh?** Misalnya, apakah pengirim menyebut adanya situasi gawat darurat yang membuatmu panik atau mengatakan bahwa dia mengenalmu, tapi **kamu tidak yakin?**

Tahukah kamu?

Safe Browsing di Chrome melindungimu dari situs berbahaya yang mungkin ingin mencuri data pribadimu **dengan memberikan peringatan** saat kamu mencoba memasuki situs tersebut.

Chrome selalu **diperbarui setiap 6 minggu sekali**, sehingga kamu selalu mendapatkan fitur dan perbaikan keamanan terbaru, serta terlindungi dari ancaman keamanan seperti malware atau phishing.

Jika kamu menemukan situs berbahaya, **laporkan kepada Google** agar kami bisa membantu menjaga internet tetap aman. Klik di sini untuk melapor.

Pertolongan pertama

Saat kamu mengalami peretasan atau pencurian perangkat, cek langkah cepat yang bisa kamu lakukan, guna memulihkan atau meminimalisir kerugian.

Tips #1

Jika akunmu diretas

Login segera dan gantilah sandimu. Bila pelaku telah mengganti sandi Akun Google-mu, ikuti langkah ini untuk memulihkannya.

Kemudian, lakukan Pemeriksaan Keamanan Google untuk melihat apakah ada akun lainnya yang turut disusupi, lalu ikuti rekomendasi yang disarankan untuk meningkatkan keamanan akun.

Tips #2

Jika ponselmu hilang atau dicuri

Kunjungi menu Temukan ponsel Anda untuk mencegah siapa pun mengakses datamu. Kamu bisa menemukan lokasi perangkat dari jarak jauh dan mengunci ponselmu (baik Android maupun iOS).

Tips Privasi Data

P3KD

Safer with Google

Saring sebelum sharing

Di era digital, kita sering berbagi informasi tanpa mempertimbangkan siapa saja yang bisa melihat konten tersebut saat itu, mau pun di masa mendatang. Simak tips berikut ini untuk memastikan kamu selalu saring sebelum sharing.

Tips #1

Jejak online-mu bisa bertahan selamanya

Setelah diposting, sulit untuk mengontrol suatu konten. Orang-orang bisa saja salah paham akan niatmu, membuat salinan (copy), menangkap layar (screenshot), atau membagikannya kembali. Maka, saringlah sebelum sharing!

Tips #2

Minta izin sebelum sharing

Apakah kamu pernah merasa kesal saat teman atau keluarga memposting foto/informasi pribadimu secara online tanpa izin?

Menghormati privasi orang lain sama pentingnya dengan menjaga privasimu. Maka, pastikan kamu selalu minta izin orang lain, sebelum membagikan konten yang melibatkan mereka, contoh: kontak, foto, berita kehamilan, wajah anak-anak, dll.

Batasi akses aplikasi dan layanan ke datamu

Produk seperti Google Maps, Search, dan YouTube memerlukan data agar layanannya lebih bermanfaat. Namun, kamu punya kontrol untuk memilih data yang ingin dibagikan. Cek tips berikut.

Tetapkan tanggal kadaluarsa untuk datamu

Google menyediakan fitur hapus otomatis untuk datamu, karena kami percaya produk hanya perlu menyimpan informasi, selama masih bermanfaat untukmu.

Terdapat opsi **hapus data otomatis setiap 18 bulan** yang aktif secara default pada:

- **Histori Lokasi** saat pertama kalinya diaktifkan.
- **Aktivitas Situs & Aplikasi** pada akun-akun baru.

Kamu selalu bisa menonaktifkan fitur atau memilih periode waktu penghapusan yang berbeda.

Kunjungi Kontrol Aktivitas di akun Google-mu untuk mengatur bagaimana datamu digunakan dan disimpan.

Batasi akses aplikasi dan layanan ke datamu

Produk seperti Google Maps, Search, dan YouTube memerlukan data agar layanannya lebih bermanfaat. Namun, kamu punya kontrol untuk memilih data yang ingin dibagikan. Cek tips berikut.

Lakukan Pemeriksaan Keamanan

Pemeriksaan Keamanan bisa membantu mengecek siapa saja aplikasi pihak ketiga yang memiliki akses ke data Akun Google-mu, bahkan mungkin kamu akan menemukan beberapa aplikasi yang sudah lama tidak digunakan.

Kontrol privasimu langsung dari aplikasi yang kamu gunakan setiap hari

Semua orang punya preferensi privasi masing-masing, sehingga tidak ada satu solusi yang sama untuk semua. Maka, kami menghadirkan kontrol yang memungkinkan kamu memilih pengaturan privasi yang tepat.

Tips #1

Aktifkan mode Samaran di Chrome, Maps, Search, dan YouTube

Cukup dengan mengklik foto profilmu, kamu bisa mengaktifkan mode Samaran secara mudah.

Saat mode Samaran diaktifkan, histori browsing, cookies, dan aktivitasmu tidak akan disimpan di Akun Google-mu.

Tips #2

Kontrol datamu, langsung dari Akun Google

Kamu bisa meninjau dan menghapus aktivitas pencarianmu, mengakses kontrol privasi yang relevan langsung di Akun Google-mu dengan cepat, tanpa perlu mengunjungi halaman pengaturan terpisah.

Klik link berikut untuk mulai mengelola datamu:

Datamu di Search | Datamu di Asisten | Datamu di Maps

Kontrol privasimu langsung dari aplikasi yang kamu gunakan setiap hari

Semua orang punya preferensi privasi masing-masing, sehingga tidak ada satu solusi yang sama untuk semua. Maka, kami menghadirkan kontrol yang memungkinkan kamu memilih pengaturan privasi yang tepat.

Lakukan Pemeriksaan Privasi

Pemeriksaan Privasi memungkinkanmu memilih jenis data yang ingin disimpan di Akun Google, menentukan siapa saja yang bisa mengaksesnya, serta mengatur jenis iklan yang ingin kamu lihat.

Kamu bisa mengubah pengaturan ini kapan saja dan mengaktifkan pengingat untuk mengelola pengaturan secara berkala.

P3KD

Safer with Google