

# Tips Menjaga Keamanan Data Pribadi Secara Digital

Oleh Ajang Cahyariki



Dengan banyaknya penggunaan internet serta media sosial dalam kehidupan sehari-hari, kasus penipuan hingga pencurian online kerap kali terjadi. Untuk menghindari hal tersebut, setiap orang harus melindungi data-data pribadinya di internet. Data pribadi yang dimaksud, setiap data tentang seseorang baik yang teridentifikasi dan/ atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung ataupun tidak langsung melalui Sistem Elektronik dan/ atau nonelektronik.

Perlu diwaspadai, ada jenis data yang sering disalahgunakan oleh pihak lain: data sukarela yang diberikan, data hasil observasi, dan data yang disimpulkan. Data sukarela yaitu data yang diberikan secara sukarela ke platform online, seperti yang kita lakukan saat registrasi ke suatu layanan. Data hasil observasi adalah data yang diambil dari aktivitas online seseorang seperti riwayat peramban serta lokasi GPS. Kemudian data yang disimpulkan merupakan gabungan dari dua jenis data sebelumnya. Ketiga jenis data itu sangat berharga, terutama untuk perusahaan-perusahaan digital yang membutuhkan banyak data untuk meningkatkan produknya.

Di era digital seperti sekarang, data adalah segalanya. Pada saat seseorang menikmati

suatu layanan digital secara gratis, disadari atau tidak, dapat dipastikan mereka membayarnya dengan data. Pada saat ini data pribadi digital belum dianggap penting oleh masyarakat Indonesia. Hal ini menjadi sebuah masalah ketika layanan digital sudah mengepung semua lapisan hidup masyarakat mulai dari layanan komunikasi hingga layanan kebutuhan sehari-hari. Kurangnya pengetahuan dan kecakapan dalam menggunakan media digital dapat dimanfaatkan dan disalahgunakan oleh beberapa pihak yang dapat mencuri dan menyalahgunakan data pribadi yang bukan miliknya. Sebagian besar masyarakat masih kesulitan membedakan mana data yang dapat disebar ke publik dan mana yang tidak. Bahkan dengan menelusuri mesin pencari saja, seseorang dapat menemukan data pribadi seperti NIK dan KK.

Seiring banyaknya penggunaan internet dan media sosial dalam kehidupan sehari-hari, kasus penipuan hingga pencurian online sering terjadi. Untuk menghindarinya, seseorang harus dapat melindungi data-data pribadinya di internet. Berikut beberapa tips untuk mengamankan data pribadi supaya tidak diretas.

## **1.Rutin Ganti Password**

Lakukanlah penggantian password pada akun aplikasi atau platform anda secara berkala dengan menggunakan password yang kuat dan unik terdiri dari gabungan nomor huruf kapital dan lain sebagainya yang tidak mudah ditebak.

## **2.Gunakan Verifikasi Dua Langkah**

Pilihlah keamanan berganda terhadap informasi data pribadi yang diberikan. Verifikasi dua langkah atau Two-factor authentication (2FA) yang ditawarkan pihak aplikasi merupakan salah satu cara melindungi data.

## **3.Jangan Menggunakan WiFi Publik**

Usahakan untuk tetap menggunakan jaringan internet pribadi dalam gadget anda. Hindari untuk menggunakan wiFi publik yang disediakan gratis demi keamanan data pribadi anda.

## **4.Selalu Update Antivirus**

Selalu memasang AntiVirus ter-update dalam gadget anda untuk mencegah masuknya malware. Antivirus akan bekerja untuk melindungi data pribadi Anda.

## **5.Lakukan Transaksi di Platform Terpercaya**

Harus mulai selektif dalam memberikan data pribadi dalam platform. Biasakan diri untuk selalu mengecek lebih dulu jenis platform yang meminta data pribadi, apakah terpercaya atau tidak untuk menghindari kebocoran data.

## **6.Gunakan Password yang Berbeda**

Apabila memiliki beberapa platform yang meminta data pribadi, selalu gunakan password yang berbeda di masing-masing platform. Baik e-commerce ataupun media sosial.

## **7.Jangan Asal Klik Link Asing**

Jangan langsung mengeklik link asing sembarangan. Sebab ditakutkan adanya phishing melalui data pribadi yang ada di patform. Phising adalah metode untuk melakukan penipuan dengan cara mengelabui target dengan maksud untuk mencuri akun target. Dengan kata lain yaitu mencuri informasi penting dengan mengambil alih akun korban untuk maksud tertentu. Biasanya hal ini dilakukan untuk mencari celah pada beberapa akun yang terhubung. Phising sering digunakan pada email, di mana penyebaran dilakukan untuk memberikan informasi yang mengarah ke halaman palsu untuk maksud menjebak korban.

## **8.Jaga Kode OTP**

Jangan pernah memberitahukan kode OTP (One-Time Password) kepada siapapun. Kode OTP umumnya dikirimkan melalui sms atau email. Anda dilarang keras untuk memberitahukan kode OTP yang anda dapatkan meskipun kepada staf/ karyawan paltform/ aplikasi yang sedang digunakan.

**“Data pribadi mempunyai nilai ekonomi yang tinggi secara agregat. Mengetahui dan melindungi data pribadi adalah suatu keharusan!!”**