**Copyright © September 2023**

# PERTEMUAN 3
# MELINDUNGI DATA DAN PRIVASI ANDA

Bab ini berfokus pada perangkat pribadi Anda dan data pribadi Anda. Ini mencakup tip untuk melindungi perangkat Anda, membuat kata sandi yang kuat, dan menggunakan jaringan nirkabel dengan aman. Ini juga membahas menjaga data Anda dengan aman. Data online Anda berharga bagi penjahat cyber. Bab ini secara singkat membahas teknik otentikasi untuk membantu Anda menjaga data Anda dengan aman. Ini juga mencakup cara untuk meningkatkan keamanan data online Anda dengan tips tentang apa yang harus dilakukan dan apa yang tidak boleh dilakukan secara online.

## 1.1. MELINDUNGI DATA ANDA

### 1.1.1. Melindungi Perangkat dan Jaringan Anda

### 1. Lindungi Perangkat Komputasi Anda

Perangkat komputasi Anda menyimpan data Anda dan merupakan portal ke kehidupan online Anda. Di bawah ini adalah daftar singkat langkah-langkah yang dapat Anda ambil untuk melindungi perangkat komputasi Anda dari gangguan:

a. Biarkan Firewall Tetap Aktif

Baik itu firewall perangkat lunak atau firewall perangkat keras pada router, firewall harus diaktifkan dan diperbarui untuk mencegah peretas mengakses data pribadi atau perusahaan Anda. Klik Windows 7 dan 8.1 atau Windows 10 untuk mengaktifkan firewall di masing-masing versi Windows. Klik di sini untuk mengaktifkan firewall untuk perangkat Mac OS X.

**Copyright © September 2023**

b. Gunakan Antivirus dan Antispyware

Perangkat lunak berbahaya, seperti virus, Trojan horse, worm, ransomware, dan spyware, diinstal pada perangkat komputasi Anda tanpa izin Anda, untuk mendapatkan akses ke komputer dan data Anda. Virus dapat merusak data Anda, memperlambat komputer Anda, atau mengambil alih komputer Anda. Salah satu cara virus dapat mengambil alih komputer Anda adalah dengan mengizinkan spammer untuk menyiarkan email menggunakan akun Anda. Spyware dapat memantau aktivitas online Anda, mengumpulkan informasi pribadi Anda, atau menghasilkan iklan pop-up yang tidak diinginkan di browser web Anda saat Anda online. Aturan yang baik adalah hanya mengunduh perangkat lunak dari situs web tepercaya untuk menghindari spyware. Perangkat lunak antivirus dirancang untuk memindai komputer Anda dan email masuk dari virus dan menghapusnya. Terkadang perangkat lunak antivirus juga menyertakan antispyware.

c. Kelola Sistem Operasi dan Peramban Anda

Peretas selalu mencoba memanfaatkan kerentanan di sistem operasi dan peramban web Anda. Untuk melindungi komputer dan data Anda, atur pengaturan keamanan di komputer dan browser Anda pada medium atau lebih tinggi. Perbarui sistem operasi komputer Anda termasuk browser web Anda dan unduh dan instal patch perangkat lunak terbaru dan pembaruan keamanan secara teratur dari vendor.

d. Kelola Sistem Operasi dan Peramban Anda

Peretas selalu mencoba memanfaatkan kerentanan di sistem operasi dan peramban web Anda. Untuk melindungi komputer dan data Anda, atur pengaturan keamanan di komputer dan browser Anda pada medium atau lebih tinggi. Perbarui sistem operasi

**Copyright © September 2023**

komputer Anda termasuk browser web Anda dan unduh dan instal patch perangkat lunak terbaru dan pembaruan keamanan secara teratur dari vendor.

e. Lindungi Semua Perangkat Anda

Perangkat komputasi Anda, baik itu PC, laptop, tablet, atau smartphone, harus dilindungi kata sandi untuk mencegah akses yang tidak sah. Informasi yang disimpan harus dienkripsi, terutama untuk data sensitif atau rahasia. Untuk perangkat seluler, simpan hanya informasi yang diperlukan, jika perangkat ini dicuri atau hilang saat Anda jauh dari rumah. Jika salah satu perangkat Anda disusupi, penjahat mungkin memiliki akses ke semua data Anda melalui penyedia layanan penyimpanan cloud Anda, seperti iCloud atau Google drive.

Perangkat IoT menimbulkan risiko yang lebih besar daripada perangkat komputasi Anda yang lain. Meskipun platform desktop, laptop, dan seluler sering menerima pembaruan perangkat lunak, sebagian besar perangkat IoT masih memiliki firmware aslinya. Jika kerentanan ditemukan di firmware, perangkat IoT kemungkinan akan tetap rentan. Untuk memperburuk masalah, perangkat IoT sering dirancang untuk menelepon ke rumah dan memerlukan akses Internet. Untuk menjangkau Internet, sebagian besar produsen perangkat IoT mengandalkan jaringan lokal pelanggan. Hasilnya adalah bahwa perangkat IoT sangat mungkin terdiri dan ketika mereka, mereka memungkinkan akses ke jaringan dan data lokal pelanggan. Cara terbaik untuk melindungi diri Anda dari skenario ini adalah dengan memiliki perangkat IoT menggunakan jaringan yang terisolasi, hanya membagikannya dengan perangkat IoT lainnya.

**Copyright © September 2023**

## 2. Gunakan Jaringan Nirkabel dengan Aman

Jaringan nirkabel memungkinkan perangkat berkemampuan Wi-Fi, seperti laptop dan tablet, untuk terhubung ke jaringan melalui pengenal jaringan, yang dikenal sebagai Service Set Identifier (SSID). Untuk mencegah penyusup memasuki jaringan nirkabel rumah Anda, SSID yang telah ditentukan sebelumnya dan kata sandi default untuk antarmuka administratif berbasis browser harus diubah. Peretas akan mengetahui informasi akses default semacam ini. Opsional, router nirkabel juga dapat dikonfigurasi untuk tidak menyiarkan SSID, yang menambahkan penghalang tambahan untuk menemukan jaringan. Namun, ini tidak boleh dianggap sebagai keamanan yang memadai untuk jaringan nirkabel. Selanjutnya, Anda harus mengenkripsi komunikasi nirkabel dengan mengaktifkan keamanan nirkabel dan fitur enkripsi WPA2 pada router nirkabel. Bahkan dengan enkripsi WPA2 diaktifkan, jaringan nirkabel masih bisa rentan.

Pada Oktober 2017, celah keamanan dalam protokol WPA2 ditemukan. Cacat ini memungkinkan penyusup untuk memecahkan enkripsi antara router nirkabel dan klien nirkabel, dan memungkinkan penyusup untuk mengakses dan memanipulasi lalu lintas jaringan. Kerentanan ini dapat dimanfaatkan dengan menggunakan K ey R einstallation A tta cks (KRACK). Ini memengaruhi semua jaringan Wi-Fi modern yang dilindungi. Untuk mengurangi penyerang, pengguna harus memperbarui semua produk yang terpengaruh: router nirkabel dan perangkat berkemampuan nirkabel, seperti laptop dan perangkat seluler, segera setelah pembaruan keamanan tersedia. Untuk laptop atau perangkat lain dengan NIC kabel, koneksi kabel dapat mengurangi kerentanan ini. Selain itu, Anda juga dapat menggunakan layanan VPN tepercaya untuk mencegah akses tidak sah ke data Anda saat Anda menggunakan jaringan nirkabel.

**Copyright © September 2023**

Saat Anda jauh dari rumah, hot spot Wi-Fi publik memungkinkan Anda mengakses informasi online dan menjelajahi Internet. Namun, yang terbaik adalah tidak mengakses atau mengirim informasi pribadi yang sensitif melalui jaringan nirkabel publik. Verifikasi apakah komputer Anda dikonfigurasi dengan berbagi file dan media dan memerlukan otentikasi pengguna dengan enkripsi. Untuk mencegah seseorang mencegat informasi Anda (dikenal sebagai "menguping") saat menggunakan jaringan nirkabel publik, gunakan terowongan dan layanan VPN terenkripsi. Layanan VPN memberi Anda akses aman ke Internet, dengan koneksi terenkripsi antara komputer Anda dan server VPN penyedia layanan VPN. Dengan terowongan VPN terenkripsi, bahkan jika transmisi data dicegat, itu tidak dapat diuraikan.

Banyak perangkat seluler, seperti ponsel cerdas dan tablet, dilengkapi dengan protokol nirkabel Bluetooth. Kemampuan ini memungkinkan perangkat berkemampuan Bluetooth untuk terhubung satu sama lain dan berbagi informasi. Sayangnya, Bluetooth dapat dimanfaatkan oleh peretas untuk menguping pada beberapa perangkat, membuat kontrol akses jarak jauh, mendistribusikan malware, dan menguras baterai. Untuk menghindari masalah ini, matikan Bluetooth saat Anda tidak menggunakannya.

### 3. Gunakan Kata Sandi Unik untuk Setiap Akun Online

Anda mungkin memiliki lebih dari satu akun online, dan setiap akun harus memiliki kata sandi yang unik. Itu banyak kata sandi yang harus diingat. Namun, konsekuensi dari tidak menggunakan kata sandi yang kuat dan unik membuat Anda dan data Anda rentan terhadap penjahat cyber. Menggunakan kata sandi yang sama untuk semua akun online Anda seperti menggunakan kunci yang sama untuk semua pintu Anda yang terkunci, jika penyerang ingin mendapatkan kunci Anda, dia akan memiliki kemampuan untuk mengakses semua yang Anda

miliki. Jika penjahat mendapatkan kata sandi Anda melalui phishing misalnya, mereka akan mencoba masuk ke akun online Anda yang lain. Jika Anda hanya menggunakan satu kata sandi untuk semua akun, mereka dapat masuk ke semua akun Anda, mencuri atau menghapus semua data Anda, atau memutuskan untuk menyamar sebagai Anda.

Kami menggunakan begitu banyak akun online yang membutuhkan kata sandi yang menjadi terlalu banyak untuk diingat. Salah satu solusi untuk menghindari penggunaan kembali kata sandi atau penggunaan kata sandi yang lemah adalah dengan menggunakan pengelola kata sandi. Pengelola kata sandi menyimpan dan mengenkripsi semua kata sandi Anda yang berbeda dan kompleks. Manajer kemudian dapat membantu Anda untuk masuk ke akun online Anda secara otomatis. Anda hanya perlu mengingat kata sandi utama Anda untuk mengakses pengelola kata sandi dan mengelola semua akun dan kata sandi Anda.

Tips memilih password yang baik :

- Jangan gunakan kata atau nama kamus dalam bahasa apa pun
- Jangan gunakan salah eja umum kata-kata kamus
- Jangan gunakan nama komputer atau nama akun
- Jika memungkinkan gunakan karakter khusus, seperti ! @ # $% ^ & * ( )
- Gunakan kata sandi dengan sepuluh karakter atau lebih

**4. Gunakan Frasa Sandi yang Lebih baik**

Untuk mencegah akses fisik yang tidak sah ke perangkat komputasi Anda, gunakan frasa sandi, bukan kata sandi. Lebih mudah membuat passphrase yang panjang daripada password, karena umumnya berbentuk kalimat daripada kata. Panjang yang lebih panjang membuat frasa sandi kurang rentan terhadap serangan kamus atau brute force. Selain itu, kata sandi mungkin

**Copyright © September 2023**

lebih mudah diingat, terutama jika Anda harus sering mengganti kata sandi. Berikut adalah beberapa tips dalam memilih kata sandi atau frasa sandi yang baik:

Tips dalam memilih kata sandi yang baik:

- Pilih pernyataan yang bermakna bagi Anda
- Tambahkan karakter khusus seperti ! @ # $% ^ & * ( )
- Semakin lama semakin baik
- Hindari pernyataan umum atau terkenal, misalnya lirik dari lagu populer popular

Baru-baru ini, Institut Nasional untuk Standar dan Teknologi Amerika Serikat (NIST) menerbitkan persyaratan kata sandi yang ditingkatkan. Standar NIST dimaksudkan untuk aplikasi pemerintah tetapi juga dapat berfungsi sebagai standar untuk orang lain juga. Pedoman baru bertujuan untuk memberikan pengalaman pengguna yang lebih baik dan menempatkan beban verifikasi pengguna pada penyedia.

Ringkasan pedoman baru:

- Panjang minimum 8 karakter, tetapi tidak lebih dari 64 karakter
- Tidak ada kata sandi yang umum dan mudah ditebak, seperti kata sandi, abc123
- Tidak ada aturan komposisi, seperti harus menyertakan huruf kecil dan huruf besar serta angka
- Tingkatkan akurasi pengetikan dengan memungkinkan pengguna melihat kata sandi saat mengetik
- Semua karakter dan spasi pencetakan diperbolehkan
- Tidak ada petunjuk kata sandi

**Copyright © September 2023**

- Tidak ada kedaluwarsa kata sandi berkala atau sewenang-wenang
- Tidak ada otentikasi berbasis pengetahuan, seperti informasi dari pertanyaan rahasia bersama, data pemasaran, riwayat transaksi

Bahkan dengan akses ke komputer dan perangkat jaringan Anda diamankan, penting juga untuk melindungi dan melestarikan data Anda.

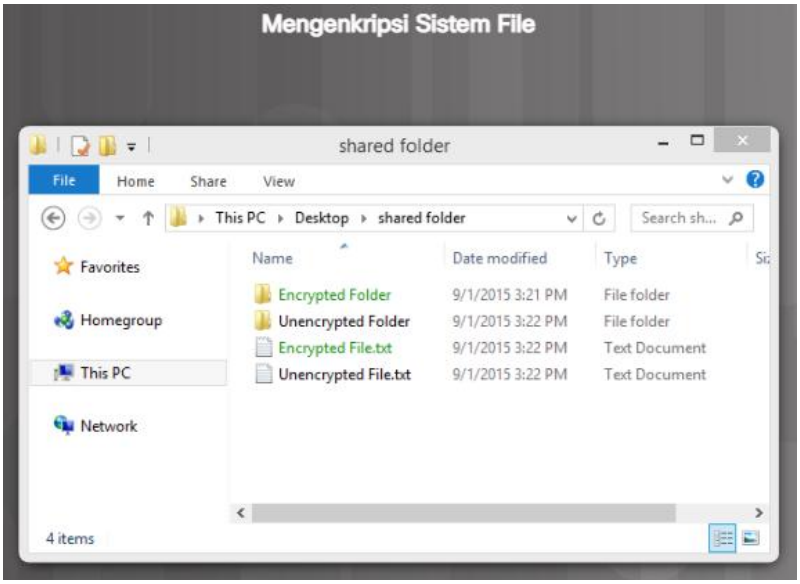
### 1.1.2. Pemeliharaan Data

#### 1. Enkripsi Data Anda

Data Anda harus selalu dienkripsi. Anda mungkin berpikir Anda tidak memiliki rahasia dan tidak ada yang disembunyikan jadi mengapa menggunakan enkripsi? Mungkin Anda berpikir bahwa tidak ada yang menginginkan data Anda. Kemungkinan besar, ini mungkin tidak benar. Apakah Anda siap untuk menunjukkan semua foto dan dokumen Anda kepada orang asing? Apakah Anda siap untuk membagikan informasi keuangan yang tersimpan di komputer Anda kepada teman-teman Anda? Apakah Anda ingin memberikan email dan kata sandi akun Anda kepada masyarakat umum? Ini bisa menjadi lebih merepotkan jika aplikasi jahat menginfeksi komputer atau perangkat seluler Anda dan mencuri informasi yang berpotensi berharga, seperti nomor akun dan kata sandi, dan dokumen resmi lainnya. Informasi semacam itu dapat menyebabkan pencurian identitas, penipuan, atau tebusan. Penjahat dapat memutuskan untuk hanya mengenkripsi data Anda dan membuatnya tidak dapat digunakan sampai Anda membayar uang tebusan. Apa itu enkripsi? Enkripsi adalah proses mengubah informasi ke dalam bentuk di mana pihak yang tidak berwenang tidak dapat membacanya. Hanya orang yang tepercaya dan berwenang dengan kunci rahasia atau kata sandi yang dapat mendekripsi data dan mengaksesnya dalam bentuk aslinya. Enkripsi itu sendiri tidak mencegah seseorang untuk

mencegat data. Enkripsi hanya dapat mencegah orang yang tidak berwenang melihat atau mengakses konten. Program perangkat lunak digunakan untuk mengenkripsi file, folder, dan bahkan seluruh drive. Encrypting File System (EFS) adalah fitur Windows yang dapat mengenkripsi data. EFS terhubung langsung ke akun pengguna tertentu. Hanya pengguna yang mengenkripsi data yang dapat mengaksesnya setelah dienkripsi menggunakan EFS. Untuk mengenkripsi data menggunakan EFS di semua versi Windows, ikuti langkah-langkah berikut:

- Langkah 1 . Pilih satu atau beberapa file atau folder.
- Langkah 2 . Klik kanan data yang dipilih >Properties .
- Langkah 3 . Klik Lanjutan…
- Langkah 4 . Pilih kotak centang Enkripsi konten untuk mengamankan data .
- Langkah 5 . File dan folder yang telah dienkripsi dengan EFS ditampilkan dalam warna hijau, seperti yang ditunjukkan pada gambar berikut




Gambar 1. Mengenkripsi Sistem File

## 2. Backup Data Anda

**Copyright © September 2023**

Hard drive Anda mungkin gagal. Laptop Anda bisa hilang. Ponsel pintar Anda dicuri. Mungkin Anda menghapus versi asli dari dokumen penting. Memiliki cadangan dapat mencegah hilangnya data yang tidak tergantikan, seperti foto keluarga. Untuk mencadangkan data dengan benar, Anda memerlukan lokasi penyimpanan tambahan untuk data tersebut dan Anda harus menyalin data ke lokasi tersebut secara berkala dan otomatis. Lokasi tambahan untuk file yang dicadangkan dapat berada di jaringan rumah, lokasi sekunder, atau di awan. Dengan menyimpan cadangan data secara lokal, Anda memiliki kendali penuh atas data tersebut. Anda dapat memutuskan untuk menyalin semua data Anda ke perangkat penyimpanan terpasang jaringan (NAS), hard drive eksternal sederhana, atau mungkin hanya memilih beberapa folder penting untuk dicadangkan pada thumb drive, CD/DVD, atau bahkan kaset. Dalam skenario itu, Anda adalah pemilik dan Anda sepenuhnya bertanggung jawab atas biaya dan pemeliharaan peralatan perangkat penyimpanan. Jika Anda berlangganan layanan penyimpanan cloud, biayanya tergantung pada jumlah ruang penyimpanan yang dibutuhkan. Dengan layanan penyimpanan cloud seperti Amazon Web Services (AWS), Anda memiliki akses ke data cadangan Anda selama Anda memiliki akses ke akun Anda. Saat Anda berlangganan layanan penyimpanan online, Anda mungkin perlu lebih selektif tentang data yang dicadangkan karena biaya penyimpanan dan transfer data online yang konstan. Salah satu manfaat menyimpan cadangan di lokasi alternatif adalah aman jika terjadi kebakaran, pencurian, atau bencana lain selain kegagalan perangkat penyimpanan.

### 3. Menghapus data secara permanen

Saat Anda memindahkan file ke recycle bin atau tempat sampah dan menghapusnya secara permanen, file tersebut hanya tidak dapat diakses dari sistem operasi. Siapa pun dengan alat forensik yang tepat masih dapat memulihkan file karena jejak magnetis yang tertinggal di hard

drive. Untuk menghapus data sehingga tidak dapat dipulihkan lagi, data harus ditimpa dengan satu dan nol beberapa kali. Untuk mencegah pemulihan file yang dihapus, Anda mungkin perlu menggunakan alat yang dirancang khusus untuk melakukan hal itu. Program SDelete dari Microsoft (untuk Vista dan lebih tinggi), mengklaim memiliki kemampuan untuk menghapus file sensitif sepenuhnya. Rusak untuk Linux dan Amankan Sampah Kosong untuk Mac OSX adalah beberapa alat yang mengklaim menyediakan layanan serupa. Satu-satunya cara untuk memastikan bahwa data atau file tidak dapat dipulihkan adalah dengan menghancurkan hard drive atau perangkat penyimpanan secara fisik. Adalah kebodohan banyak penjahat dalam berpikir bahwa file mereka tidak dapat ditembus atau tidak dapat dipulihkan. Selain menyimpan data di hard drive lokal Anda, data Anda juga dapat disimpan secara online di cloud. Salinan itu juga perlu dihapus. Luangkan waktu sejenak untuk bertanya pada diri sendiri, “Di mana saya menyimpan data saya? Apakah itu dicadangkan di suatu tempat? Apakah itu dienkripsi? Ketika Anda perlu menghapus data Anda atau membuang hard drive atau komputer, tanyakan pada diri sendiri, "Apakah saya telah mengamankan data agar tidak jatuh ke tangan yang salah?"

## 1.2. Menjaga Privasi Online Anda

### 1.2.1. Perkuat Otentikasi

#### 1. Dua Faktor Otentikasi

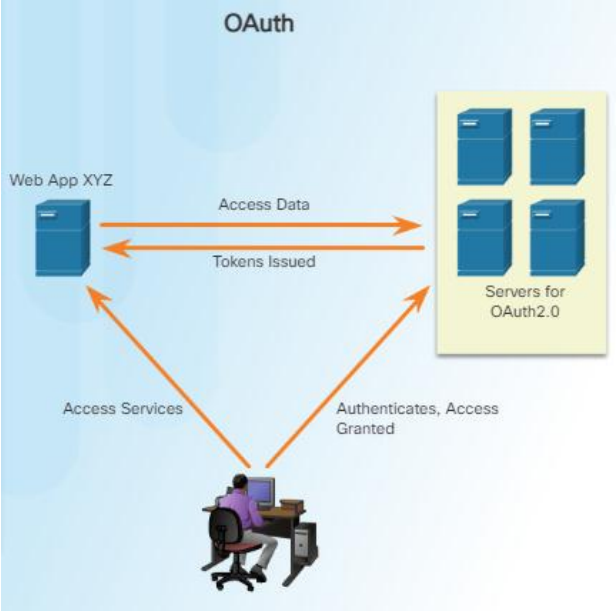
Layanan online populer, seperti Google, Facebook, Twitter, LinkedIn, Apple dan Microsoft, menggunakan otentikasi dua faktor untuk menambahkan lapisan keamanan ekstra untuk login akun. Selain nama pengguna dan kata sandi, atau nomor identifikasi pribadi (PIN) atau pola, otentikasi dua faktor memerlukan token kedua, seperti:

- Objek fisik - kartu kredit, kartu ATM, telepon, atau fob

- Pemindaian biometrik - sidik jari, sidik jari, serta pengenalan wajah atau suara

Bahkan dengan otentikasi dua faktor, peretas masih bisa mendapatkan akses ke akun online Anda melalui serangan seperti serangan phishing, malware, dan rekayasa sosial.

## 2. OAuth 2.0




gambar 2. OAuth

Open Authorization (OAuth) adalah protokol standar terbuka yang memungkinkan kredensial pengguna akhir untuk mengakses aplikasi pihak ketiga tanpa memaparkan kata sandi pengguna. OAuth bertindak sebagai perantara untuk memutuskan apakah akan mengizinkan pengguna akhir mengakses aplikasi pihak ketiga. Misalnya, Anda ingin mengakses aplikasi web XYZ, dan Anda tidak memiliki akun pengguna untuk mengakses aplikasi web ini. Namun, XYZ memiliki opsi untuk mengizinkan Anda masuk menggunakan kredensial dari situs web media sosial ABC. Jadi Anda mengakses situs web menggunakan login media sosial.

Agar ini berfungsi, aplikasi 'XYZ' terdaftar di 'ABC' dan merupakan aplikasi yang disetujui. Saat Anda mengakses XYZ, Anda menggunakan kredensial pengguna Anda untuk ABC. Kemudian XYZ meminta token akses dari ABC atas nama Anda. Sekarang Anda memiliki akses ke XYZ. XYZ tidak tahu apa-apa tentang Anda dan kredensial pengguna Anda, dan interaksi ini benar-benar mulus bagi pengguna. Menggunakan token rahasia mencegah aplikasi jahat mendapatkan informasi dan data Anda.

### 1.2.2. Informasi Yang Terlalu Banyak DiShare?

**1. Jangan Terlalu Banyak Berbagi di Media Sosial**

Jika Anda ingin menjaga privasi Anda di media sosial, bagikan informasi sesedikit mungkin. Anda tidak boleh membagikan informasi seperti tanggal lahir, alamat email, atau nomor telepon Anda di profil Anda. Orang-orang yang perlu mengetahui informasi pribadi Anda mungkin sudah mengetahuinya. Jangan mengisi profil media sosial Anda dengan lengkap, hanya berikan informasi minimum yang diperlukan. Selanjutnya, periksa pengaturan media sosial Anda untuk mengizinkan hanya orang yang Anda kenal yang melihat aktivitas Anda atau terlibat dalam percakapan Anda. Semakin banyak informasi pribadi yang Anda bagikan secara online, semakin mudah bagi seseorang untuk membuat profil tentang Anda dan memanfaatkan Anda secara offline. Pernahkah Anda lupa nama pengguna dan kata sandi untuk akun online? Pertanyaan keamanan seperti “Siapa nama gadis ibumu?” atau “Di kota mana kamu dilahirkan?” seharusnya membantu menjaga akun Anda aman dari penyusup. Namun, siapa pun yang ingin mengakses akun Anda dapat mencari jawabannya di Internet. Anda dapat menjawab pertanyaan-pertanyaan ini dengan informasi yang salah, selama Anda dapat mengingat jawaban yang salah. Jika Anda memiliki masalah dalam mengingatnya, Anda dapat menggunakan pengelola kata sandi untuk mengelolanya untuk Anda.

**Copyright © September 2023**

**2. Privasi email dan web Browser**

Setiap hari, jutaan pesan email digunakan untuk berkomunikasi dengan teman dan melakukan bisnis. Email adalah cara mudah untuk berkomunikasi satu sama lain dengan cepat. Saat Anda mengirim email, ini mirip dengan mengirim pesan menggunakan kartu pos. Pesan kartu pos ditransmisikan di depan mata siapa saja yang memiliki akses untuk melihat, dan pesan email ditransmisikan dalam teks biasa, dan dapat dibaca oleh siapa saja yang memiliki akses. Komunikasi ini juga diteruskan di antara server yang berbeda saat dalam rute ke tujuan. Bahkan ketika Anda menghapus pesan email Anda, pesan tersebut dapat diarsipkan di server email untuk beberapa waktu.

Siapa pun yang memiliki akses fisik ke komputer Anda, atau router Anda, dapat melihat situs web mana yang telah Anda kunjungi menggunakan riwayat browser web, cache, dan mungkin file log. Masalah ini dapat diminimalkan dengan mengaktifkan mode penjelajahan pribadi di browser web. Sebagian besar browser web populer memiliki nama sendiri untuk mode browser pribadi:

- Microsoft Internet Explorer : InPrivate
- Google Chrome : Penyamaran
- Mozilla Firefox : Tab pribadi / jendela pribadi
- Safari : Pribadi: Penjelajahan pribadi

**Copyright © September 2023**

Dengan mengaktifkan mode privat, cookie dinonaktifkan, dan file Internet sementara serta riwayat penelusuran dihapus setelah menutup jendela atau program. Menjaga kerahasiaan riwayat penjelajahan Internet Anda dapat mencegah orang lain mengumpulkan informasi tentang aktivitas online Anda dan memikat Anda untuk membeli sesuatu dengan iklan bertarget. Bahkan dengan penjelajahan pribadi diaktifkan dan cookie dinonaktifkan, perusahaan sedang mengembangkan berbagai cara pengguna sidik jari untuk mengumpulkan informasi dan melacak perilaku pengguna. Misalnya, perangkat perantara, seperti router, dapat memiliki informasi tentang riwayat penelusuran web pengguna. Pada akhirnya, Anda bertanggung jawab untuk melindungi data, identitas, dan perangkat komputasi Anda. Saat Anda mengirim email, haruskah Anda menyertakan catatan medis Anda? Lain kali Anda menjelajah Internet, apakah transmisi Anda aman? Hanya beberapa tindakan pencegahan sederhana yang dapat menyelamatkan Anda dari masalah nanti.