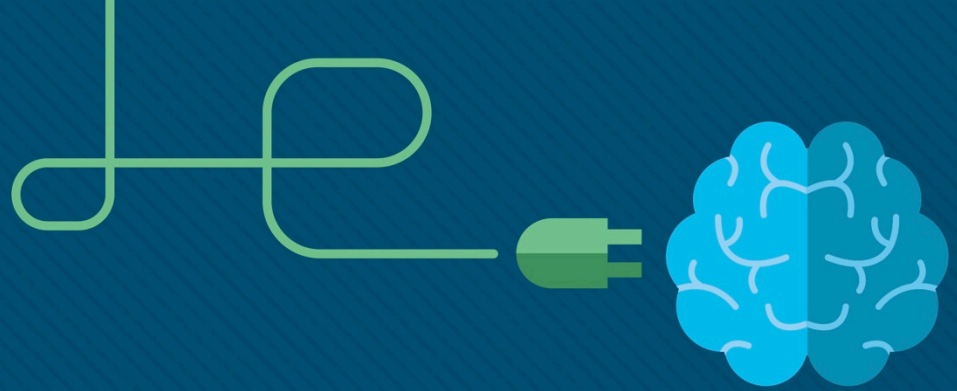


Bab 3: Melindungi Data dan Privasi Anda

Materi Instruktur

Pendahuluan Tentang Keamanan Cyber v2.1

Materi Instruktur – Bab 3 Panduan Perencanaan

- Rangkaian PowerPoint ini terbagi dalam dua bagian:
- Panduan Perencanaan Instruktur
  - Informasi yang dapat Anda gunakan untuk mempelajari semua bab
  - Alat bantu pengajaran
- Presentasi Kelas Instruktur
  - Slide opsional yang dapat Anda gunakan di kelas
  - Mulai di slide # 9

- **Catatan**: Hapus Panduan Perencanaan dari presentasi ini sebelum menampilkannya kepada semua siswa.

Bab 3: Melindungi Data dan Privasi Anda

Panduan Perencanaan Pendahuluan Tentang Keamanan Cyber v2.1

Bab 3: Aktivitas

Aktivitas apa yang terkait dengan bab ini?

Halaman #	Jenis Aktivitas	Nama Aktivitas
3.1.1.5	Lab	Membuat dan Menyimpan Kata Sandi yang Kuat
3.1.2.3	Lab	Mencadangkan Data ke Penyimpanan Eksternal
3.1.2.5	Lab	Siapa yang Memiliki Data Anda?
3.2.2.3	Lab	Mempelajari Perilaku Anda yang Memiliki Risiko Online

Bab 3: Penilaian

- Siswa harus menyelesaikan Bab 3, “Penilaian” setelah menyelesaikan Bab 3.
- Kuis, lab, dan aktivitas lainnya dapat digunakan untuk menilai kemajuan siswa secara informal.

Bab 3: Praktik Terbaik

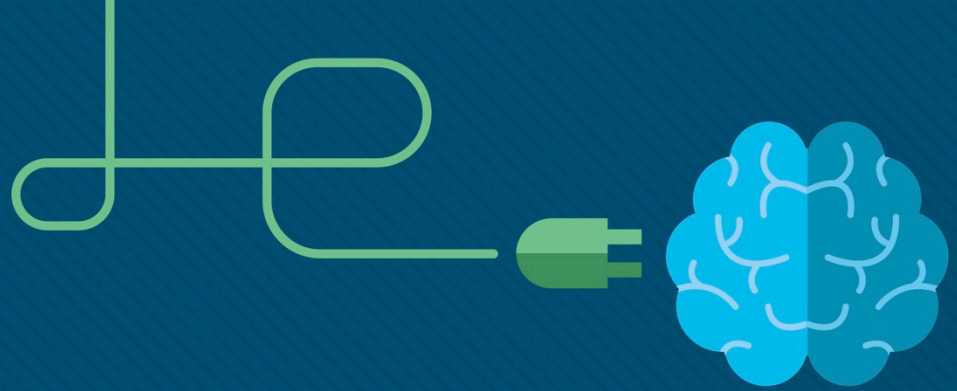
Sebelum mengajar Bab 3, instruktur harus:

- Menyelesaikan Bab 3, “Penilaian”.
- Tinjau dokumen Sumber Daya dan Aktivitas Tambahan dalam Sumber Daya Siswa untuk melihat kemungkinan sumber daya dan aktivitas tambahan.
- Sasaran bab ini adalah:
  - Menjelaskan cara melindungi perangkat dan jaringan
  - Menjelaskan prosedur yang aman untuk pemeliharaan data.
  - Menjelaskan metode otentikasi yang kuat
  - Menjelaskan perilaku online yang aman.

Bab 3: Bantuan Tambahan

- Untuk bantuan tambahan tentang strategi pengajaran, termasuk rencana pelajaran, analogi untuk konsep yang sulit, dan topik diskusi, kunjungi Forum Komunitas.
- Jika Anda memiliki rencana pelajaran atau sumber daya yang ingin dibagi, unggah ke Forum Komunitas untuk membantu instruktur lain.


CISCO



Bab 3: Melindungi Data dan Privasi Anda

Pendahuluan Tentang Keamanan Cyber v2.1

Bab 3 - Bagian & Sasaran

- 3.1 Melindungi Data Anda
  - Menjelaskan cara melindungi perangkat dari ancaman.
    - Menjelaskan cara melindungi perangkat dan jaringan.
    - Menjelaskan prosedur yang aman untuk pemeliharaan data.
- 3.2 Menjaga Keamanan Privasi Online Anda
  - Menjelaskan cara menjaga keamanan privasi.
    - Menjelaskan metode otentikasi yang kuat.
    - Menjelaskan perilaku online yang aman.

3.1 Melindungi Data Anda

Melindungi Perangkat Komputer Anda

- Selalu Aktifkan Firewall
  - Cegah akses tidak sah ke data atau perangkat komputer Anda
  - Selalu perbarui firewall
- Gunakan Antivirus dan Antispyware
  - Cegah akses tidak sah ke data atau perangkat komputer Anda
  - Hanya unduh perangkat lunak dari situs web tepercaya
  - Selalu perbarui perangkat lunak
- Kelola Sistem Operasi dan Peramban Anda
  - Tetapkan pengaturan keamanan ke sedang atau lebih tinggi
  - Perbarui sistem operasi komputer dan peramban Anda
  - Unduh serta instal patch dan pembaruan keamanan perangkat lunak terkini
- Lindungi Semua Perangkat Anda
  - Lindungi dengan kata sandi
  - Eknripsikan data
  - Hanya simpan informasi yang penting
  - Perangkat IoT

Gunakan Jaringan Nirkabel Secara Aman

- Jaringan Nirkabel Rumah
  - Ubah SSID standar dan kata sandi administratif default di router Wi-Fi.
  - Nonaktifkan siaran SSID
  - Gunakan fitur enkripsi WPA2
  - Ketahui kekurangan keamanan protokol WPA2 – KRACK
    - Penyusup dapat membuka enkripsi antara router nirkabel dan klien
- Hati-hati saat menggunakan hotspot Wi-Fi publik
  - Jangan akses atau kirim informasi sensitif
  - Penggunaan tunnel VPN dapat mencegah penyadapan
- Nonaktifkan Bluetooth bila tidak digunakan

Gunakan Kata Sandi Unik untuk Setiap Akun Online

- Mencegah pelaku kriminal mengakses semua akun online Anda menggunakan satu kredensial curian
- Gunakan pengelola kata sandi untuk membantu mengingat kata sandi
- Tips memilih kata sandi yang bagus:
  - Jangan gunakan kata dalam kamus atau nama dalam bahasa apa pun
  - Jangan gunakan kesalahan eja yang umum dari kata dalam kamus
  - Jangan gunakan nama komputer atau nama akun
  - Jika memungkinkan, gunakan karakter khusus, misalnya ! @ # $ % ^ & * ( )
  - Gunakan kata sandi dengan 10 karakter atau lebih

Oke	Baik	Lebih baik
allwhitecat	a 11 whitecat	A 11 whi7ec@t
Fblogin	1FBLogin	1FBL0gin$
amazonpass	AmazonPa55	Am@z0nPa55
ilikemyschool	ILikeMySchool	ILik3MySch00l
Hightidenow	HighTideNow	H1gh7id3now

Gunakan Kalimat Sandi dan Bukan Kata Sandi

- Tips memilih kalimat sandi yang bagus:
  - Pilih pernyataan yang bermakna untuk Anda
  - Tambahkan karakter khusus, misalnya ! @ # $ % ^ & * ( )
  - Semakin panjang semakin baik
  - Jangan gunakan pernyataan yang umum atau terkenal, misalnya lirik dari lagu populer
- Ringkasan panduan NIST baru:
  - Panjang minimum 8 karakter, maksimum 64 karakter
  - Bukan kata sandi umum yang mudah ditebak, misalnya password, abc123
  - Tidak ada aturan penyusunan, misalnya berisi huruf besar dan kecil serta angka
  - Tidak ada otentikasi berdasarkan pengetahuan, misalnya informasi dari pertanyaan rahasia bersama, data pemasaran, riwayat transaksi
  - Meningkatkan keakuratan pengetikan dengan memungkinkan pengguna melihat kata sandi saat mengetik
  - Semua karakter cetak dan spasi boleh digunakan
  - Tidak ada petunjuk kata sandi
  - Tidak ada waktu berakhir berkala atau mendadak untuk kata sandi

Oke	Thisismypassphrase
Baik	Acatthatlovesdogs
Lebih baik	Acat th@tlov3sd0gs.

Lab – Membuat dan Menyimpan Kata Sandi yang Kuat

Networking Academy

Lab – Create and Store Strong Passwords

Objectives

Understand the concepts behind a strong password.

Part 1: Explore the concepts behind creating a strong password.

Part 2: Explore the concepts behind securely storing your passwords?

Background / Scenario

Passwords are widely used to enforce access to resources. Attackers will use many techniques to learn users' passwords and gain unauthorized access to a resource or data.

To better protect yourself, it is important to understand what makes a strong password and how to store it securely.

Required Resources

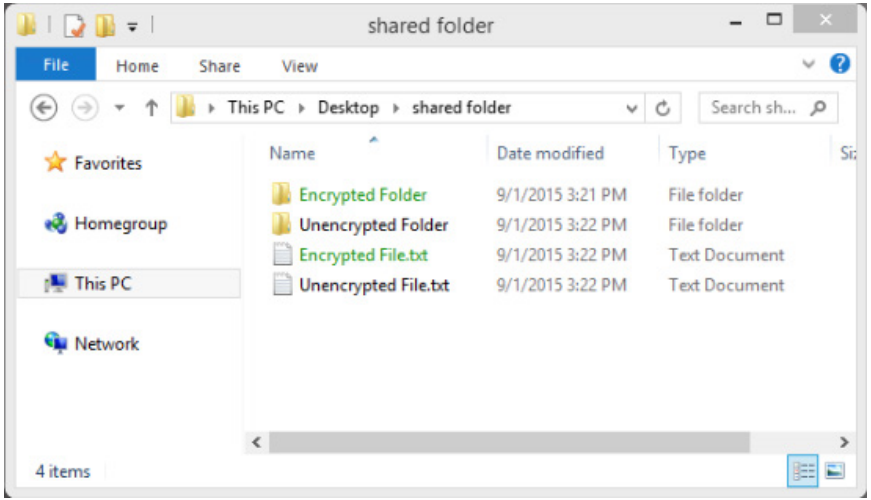
- PC or mobile device with Internet access

Part 1: Creating a Strong Password

Strong passwords have four main requirements listed in order of importance:

Enkripsikan Data Anda

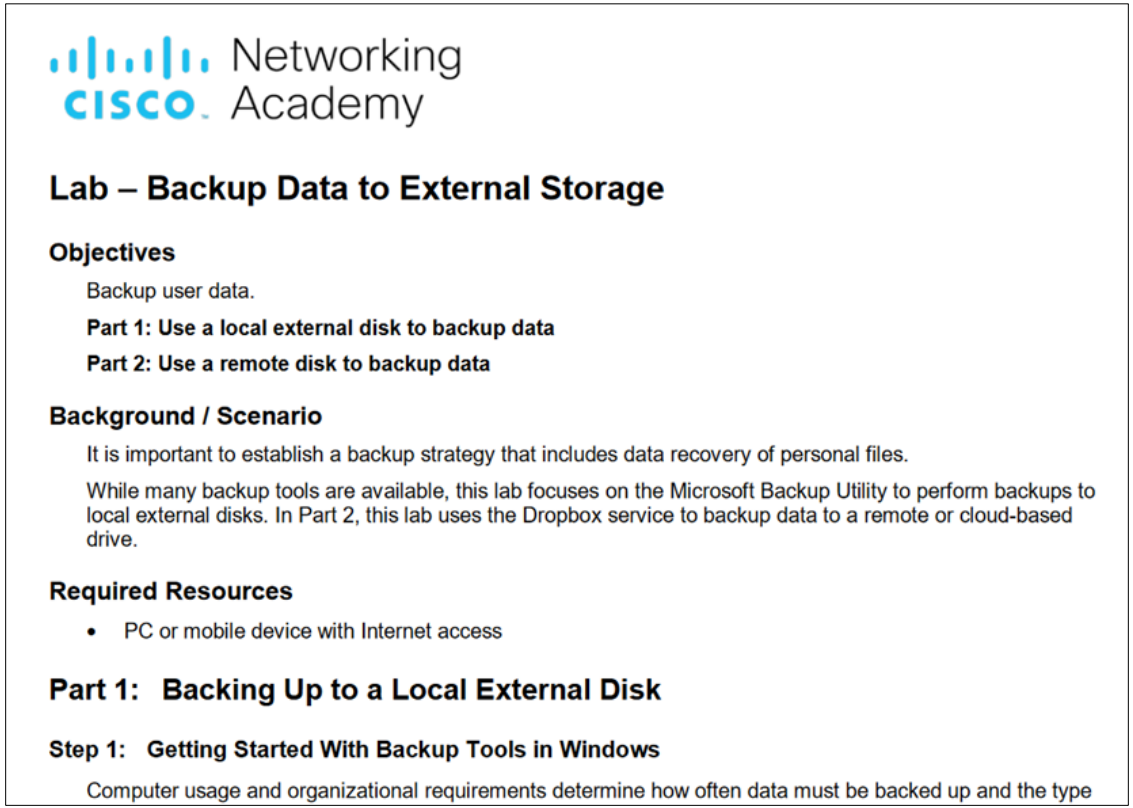
- Data yang dienkripsi hanya dapat dibaca dengan kode rahasia atau kata sandi
- Cegah pengguna yang tidak sah membaca konten
- Apa Itu Enkripsi?
  - proses konversi informasi ke dalam bentuk yang tidak dapat dibaca oleh pihak yang tidak sah



Cadangkan Data Anda

- Mencegah hilangnya data yang sangat penting
- Memerlukan lokasi penyimpanan tambahan untuk data
- Salin data ke lokasi pencadangan secara terjadwal dan otomatis
- Pencadangan Lokal
  - NAS, hard drive eksternal, CD/DVD, flash drive, atau pita magnetik
  - Kontrol dan tanggung jawab penuh atas biaya dan pemeliharaan
- Layanan Penyimpanan Cloud, misalnya AWS
  - Cadangan dapat diakses selama Anda dapat mengakses akun Anda
  - mungkin harus menyeleksi data yang akan dicadangkan

Lab – Mencadangkan Data ke Penyimpanan Eksternal



Networking Academy

Lab – Backup Data to External Storage

Objectives

Backup user data.

Part 1: Use a local external disk to backup data

Part 2: Use a remote disk to backup data

Background / Scenario

It is important to establish a backup strategy that includes data recovery of personal files.

While many backup tools are available, this lab focuses on the Microsoft Backup Utility to perform backups to local external disks. In Part 2, this lab uses the Dropbox service to backup data to a remote or cloud-based drive.

Required Resources

- PC or mobile device with Internet access

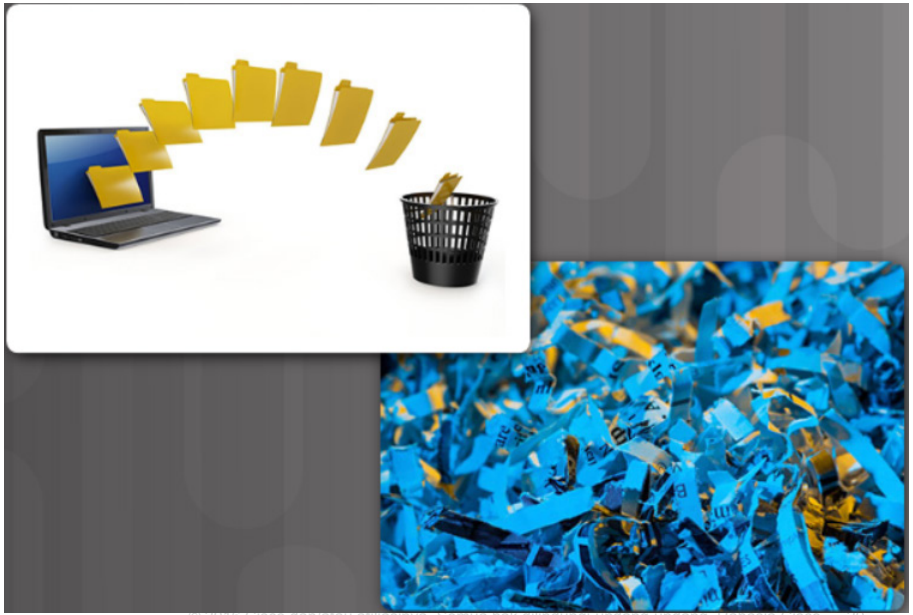
Part 1: Backing Up to a Local External Disk

Step 1: Getting Started With Backup Tools in Windows

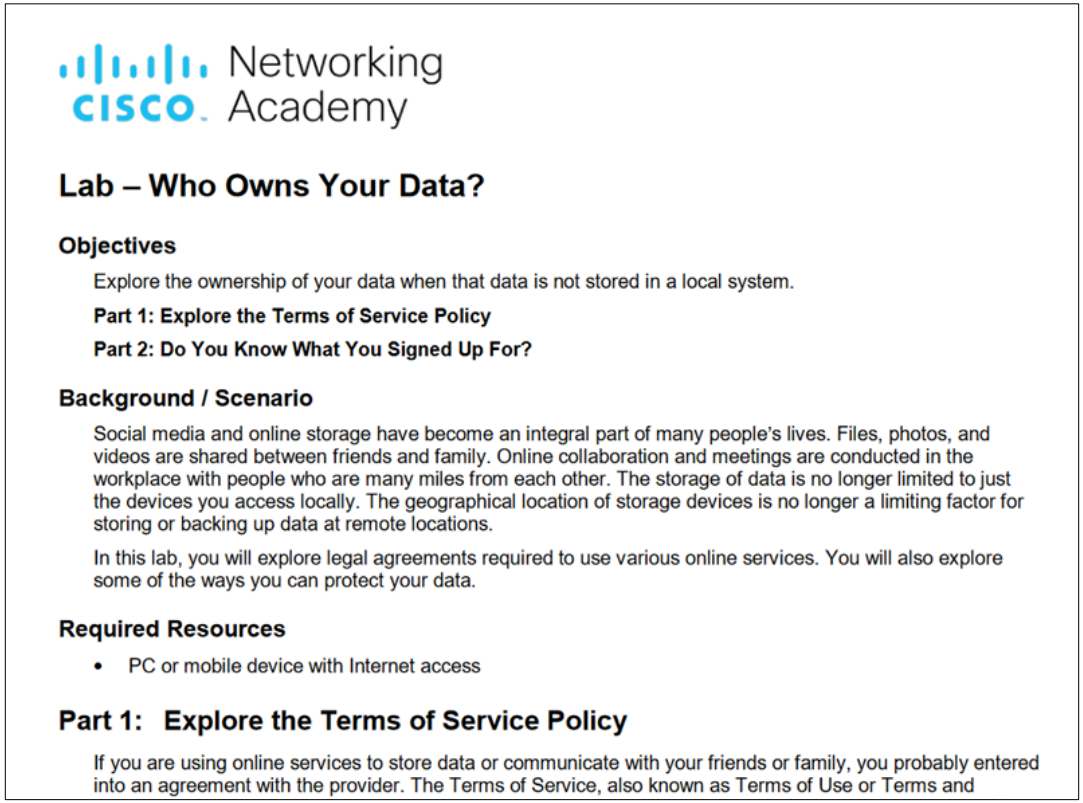
Computer usage and organizational requirements determine how often data must be backed up and the type

Menghapus Data Secara Permanen

- Gunakan alat bantu yang tersedia untuk menghapus data secara permanen: misalnya SDelete dan Secure Empty Trash
- Hancurkan perangkat penyimpanan untuk memastikan data tidak dapat dipulihkan
- Hapus versi online



Lab – Siapa yang Memiliki Data Anda?



Networking Academy

Lab – Who Owns Your Data?

Objectives

Explore the ownership of your data when that data is not stored in a local system.

Part 1: Explore the Terms of Service Policy

Part 2: Do You Know What You Signed Up For?

Background / Scenario

Social media and online storage have become an integral part of many people's lives. Files, photos, and videos are shared between friends and family. Online collaboration and meetings are conducted in the workplace with people who are many miles from each other. The storage of data is no longer limited to just the devices you access locally. The geographical location of storage devices is no longer a limiting factor for storing or backing up data at remote locations.

In this lab, you will explore legal agreements required to use various online services. You will also explore some of the ways you can protect your data.

Required Resources

- PC or mobile device with Internet access

Part 1: Explore the Terms of Service Policy

If you are using online services to store data or communicate with your friends or family, you probably entered into an agreement with the provider. The Terms of Service, also known as Terms of Use or Terms and

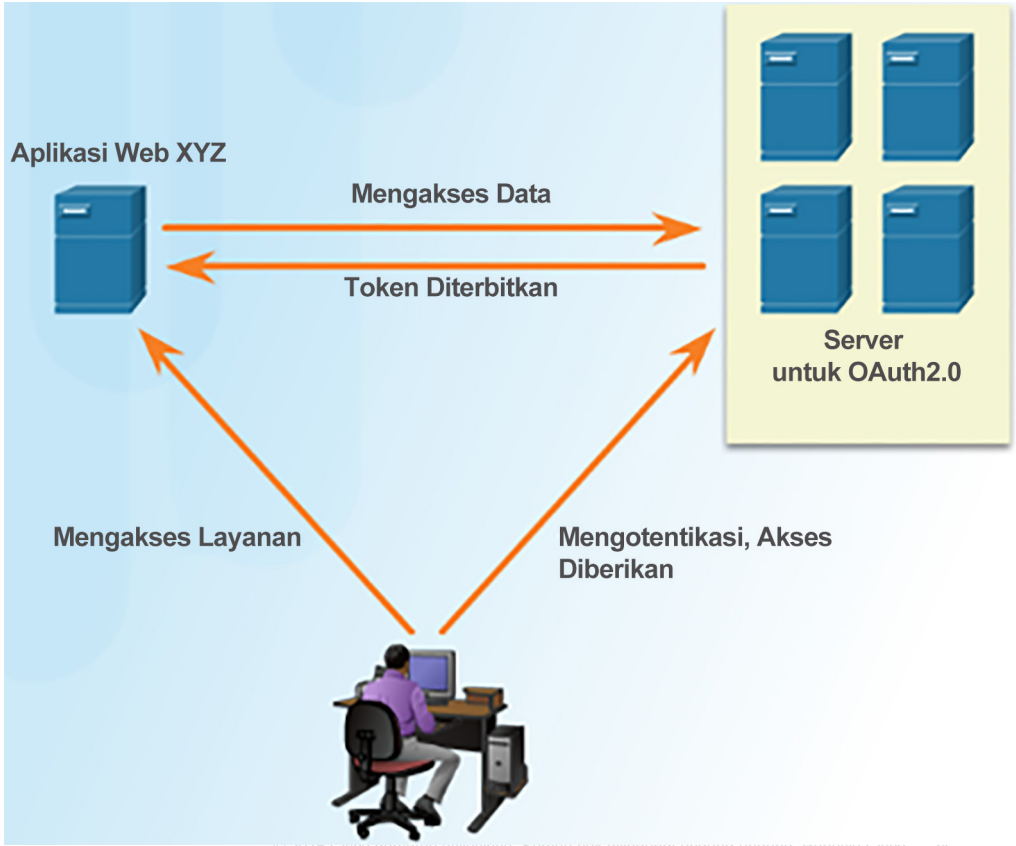
3.2 Menjaga Keamanan Privasi Online Anda

Otentikasi Dua Faktor

- Layanan online populer menggunakan otentikasi dua faktor
- Memerlukan Nama pengguna/kata sandi atau PIN dan token kedua untuk mengakses:
  - **Objek fisik** - kartu kredit, kartu ATM, ponsel, atau fob
  - **Pemindaian biometrik** - pemindaian sidik jari, pemindaian telapak tangan, dan pengenalan wajah atau suara

OAuth 2.0

- Protokol standar terbuka yang memungkinkan kredensial pengguna akhir mengakses aplikasi pihak ketiga tanpa mengungkapkan kata sandi pengguna
- Bertindak sebagai perantara untuk memutuskan apakah akan membolehkan pengguna akhir mengakses aplikasi pihak ketiga.



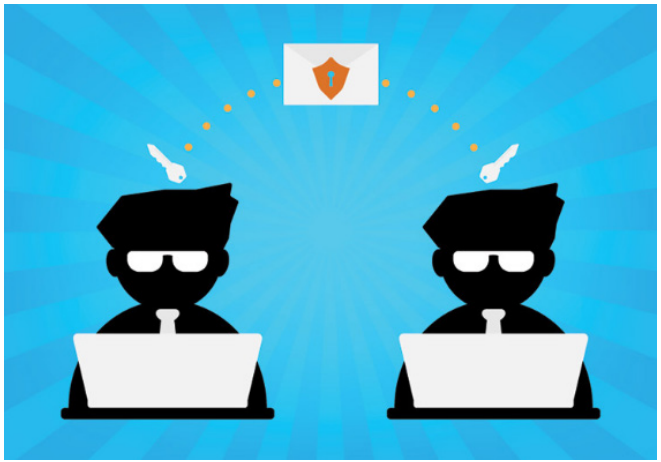
Jangan Bagi Terlalu Banyak Informasi di Media Sosial

- Bagikan sesedikit mungkin informasi di media sosial
- Jangan bagikan informasi seperti:
  - Tanggal lahir
  - Alamat email
  - Nomor telepon
- Periksa pengaturan media sosial Anda

Berbagi Terlalu Banyak Informasi?

Privasi Email dan Peramban Web

- Email mirip seperti mengirimkan kartu pos.
- Salinan email dapat dibaca oleh siapa pun yang dapat mengaksesnya.
- Email dikirim melalui berbagai server
- Gunakan mode penelusuran rahasia yang dapat mencegah orang lain mengumpulkan informasi tentang aktivitas online Anda.
- Mode rahasia di peramban populer
  - **Microsoft Internet Explorer**: InPrivate
  - **Google Chrome**: Incognito
  - **Mozilla Firefox**: Tab/jendela rahasia
  - **Safari**: Private: Private browsing



Lab – Pelajari Perilaku Anda yang Memiliki Risiko Online

Networking Academy

Lab – Discover Your Own Risky Online Behavior

Objectives

Explore actions performed online that may compromise your safety or privacy.

Background / Scenario

The Internet is a hostile environment, and you must be vigilant to ensure your data is not compromised. Attackers are creative and will attempt many different techniques to trick users. This lab helps you identify risky online behavior and provide tips on how to become safer online.

Part 1: Explore the Terms of Service Policy

Answer the questions below with honesty and take note of how many points each answer gives you. Add all points to a total score and move on to Part 2 for an analysis of your online behavior.

a. What kind of information do you share with social media sites?

1) Everything; I rely on social media to keep in touch with friends and family. (3 points)
2) Articles and news I find or read (2 points)
3) It depends; I filter out what I share and with whom I share. (1 point)
4) Nothing; I do not use social media. (0 points)

3.3 Ringkasan Bab

Ringkasan

- Menjelaskan cara melindungi perangkat dan jaringan dari ancaman.
- Menjelaskan prosedur yang aman untuk pemeliharaan data.
- Menjelaskan cara menjaga keamanan privasi Anda menggunakan metode otentikasi yang kuat dan dengan mempraktikkan perilaku online yang aman.


CISCO