Berpartisipasilah secara online dengan aman dan bertanggungjawab

26 menit

Di jalur pembelajaran ini, Anda akan diperkenalkan tentang resiko keamanan yang bisa Anda hadapi ketika menggunakan internet. Anda akan belajar tentang scam online (penipuan online) dan bagaimana cara menghindarinya. Anda juga akan belajar tentang cara terbaik di dalam membagikan informasi di internet. Selain itu, Anda juga akan diperkenalkan tentang intimidasi melalui internet alias cyberbullying.

# Keamanan dan privasi di internet

17 menit | 8 unit

Di modul ini, Anda akan belajar tentang beberapa resiko keamanan yang bisa mempengaruhi Anda ketika Anda sedang menggunakan internet, dan petunjuk agar tetap aman, dan menjaga privasi informasi Anda di internet.

## Lindungi diri Anda dari phishing

3 menit

### Lindungi diri Anda dari phishing (penipuan identitas demi mendapatkan data pribadi)

Meskipun ada banyak perbuatan baik yang bisa kita lakukan di internet, tetapi kita harus selalu sadar akan adanya resiko keamanan. Ada banyak scam (penipuan) yang digunakan oleh para pemangsa di internet untuk masuk ke data masyarakat melalui internet.

Anda harus menyadari berbagai scam ini supaya Anda bisa berusaha semampu Anda untuk menghindarinya. Phishing merupakan scam umum di internet yang harus Anda sadari.

**Saksikan video di bawah ini untuk belajar lebih banyak lagi tentang phishing dan bagaimana melindungi diri Anda dari scam online ini.**

### [Video: Lindungi diri Anda dari phishing](https://www.microsoft.com/en-us/videoplayer/embed/RWtIc4)

Internet mendatangkan banyak kemungkinan untuk kita. Kita bisa berbicara dengan oranglain, melakukan pembelian online, dan melakukan bisnis pribadi dari satu tempat. Tetapi, interaksi online ini tidak selalu aman. Mari kita membicarakan scam online yang populer yang harus Anda sadari.

Salah satu cara yang umum digunakan untuk menangkap ikan adalah dengan meletakkan umpan ke kail agar ikannya mau memakan umpannya. Setelah ikannya menggigit umpannya, ikannya akan terkait. Scam berjenis phishing di internet bekerja dengan cara serupa. Orang-orang yang ingin mencuri informasi Anda itu seperti pemancing ikan. Mereka akan mengirimkan email atau pesan singkat melalui situs media social atau permainan online. Mereka sering berpura-pura menjadi seseorang yang bukan diri mereka yang sebenarnya, dan meminta informasi pribadi, atau mereka meminta Anda mengklik hyperlink agar Anda bisa menyelesaikan suatu tugas penting. Jika Anda memberi mereka informasi, atau mengklik hyperlink, maka Anda akan terkait. Tetapi, jangan khawatir. 4 (empat) cara ini bisa menolong melindungi Anda dari penipuan (scam) berjenis phishing (penipuan identitas demi mendapatkan data pribadi).

Cara nomor 1 (satu). Waspadalah terhadap pesan yang mencurigakan. Para penipu mencoba membuat pesan mereka tampak resmi dan familiar agar Anda mempercayainya. Berpikirlah dua kali ketika Anda menerima pesan yang mencurigakan, dan hindari berbagi informasi pribadi melalui pesan atau email. Ini termasuk alamat rumah, informasi bank, kode sandi, dan informasi lain yang Anda miliki. Jangan mengklik di tautan (link) atau mendownload file jika Anda tidak mengenal atau tidak mempercayai pengirimnya.

Cara nomor 2 (dua). Carilah tanda yang menunjukkan bahwa halaman web-nya aman. Sebelum Anda menyediakan info kartu kredit, masukkan kata sandi, atau sediakan info pribadi lainnya, verifikasi bahwa Anda berada di situs web aman terpercaya. Sebagian besar situs web diawali dengan https di awal URL di address bar (papan alamat) browser-nya. Selain itu, pastikan bahwa Anda berada di halaman web yang benar. Para penipu sering mencoba mengarahkan Anda ke halaman web yang tampak resmi, dan menggunakan perusahaan yang namanya salah eja untuk mengakal-akali Anda. www.microsoft.net tidak sama dengan situs web resmi milik Microsoft di [www.microsoft.com](http://www.microsoft.com).

Periksa senantiasa URL-nya untuk memastikan bahwa Anda berada di situs web yang benar.

Cara nomor 3 (tiga). Selalu memperbarui browser web dan system operasi Anda. Anda bisa mengaktifkan pembaruan otomatis untuk memastikan terbitan perangkat lunak terbaru terpasang otomatis ke komputer Anda. Dengan selalu memperbarui perangkat lunak di perangkat Anda berarti Anda akan menerima pembaruan keamanan terbaru yang menolong melindungi komputer Anda.

Cara nomor 4 (empat). Pasanglah perangkat lunak anti-malware terverifikasi ke perangkat Anda. Ini merupakan perangkat lunak khusus yang didesain untuk melindungi komputer Anda dari perangkat lunak berbahaya dan hacker. Jangan menjadi ikan selanjutnya yang terkait. Ketika Anda menggunakan internet, jangan lupa berpikir sebelum Anda mengklik, mendownload, atau berbagi untuk melindungi diri Anda dari penipuan phishing online.

## Berkomunikasi online dengan aman

2 menit

### Berkomunikasi online dengan aman

Internet memudahkan Anda berkomunikasi online dengan oranglain. Anda tidak selalu tahu pasti siapa yang berbicara dengan Anda ketika Anda berada di internet sehingga Anda harus waspada agar tetap aman.

**Saksikan video di bawah ini untuk belajar bagaimana berkomunikasi online dengan aman.**

### [Video: Berkomunikasi online dengan aman](https://www.microsoft.com/en-us/videoplayer/embed/RWtD0y)

Dengan menggunakan internet, kita bisa berkomunikasi dengan oranglain lintas negara dengan cara baru. Ini banyak manfaatnya, tetapi ada juga beberapa resiko. Ada pemangsa online yang menggunakan internet setiap hari. Pemangsa ini sering berpura-pura menjadi oranglain yang bukan dirinya. Jadi, mungkin sulit mengenali dengan siapa Anda berbicara di internet. Ini merupakan 3 (tiga) petunjuk yang bisa Anda gunakan untuk membuat diri Anda tetap aman dari pemangsa di internet ketika Anda sedang berkomunikasi di internet.

Petunjuk nomor 1 (satu). Gunakan naluri Anda. Jika seseorang membuat Anda merasa gelisah atau tidak nyaman, maka berhentilah berkomunikasi dengannya, dan segera ceritakanlah ke orang yang Anda percayai. Sebagian besar situs web dan situs media social mempunyai alat-alat yang bisa Anda gunakan untuk melaporkan kegiatan yang mencurigakan.

Petunjuk nomor 2 (dua). Batasi apa yang Anda bagikan. Pemangsa online sering mencoba menangkap Anda untuk membagikan informasi pribadi Anda melalui email dan pesan. Hindari berbagi informasi pribadi ke orang asing di internet.

Petunjuk nomor 3 (tiga). Jaga jarak Anda. Berpikirlah dua kali sebelum menemui secara pribadi seseorang yang barusan berbicara dengan Anda di internet. Pemangsa online sering menggunakan media social untuk berpura-pura menjadi seseorang yang bukan dirinya dengan mengatur profil palsu dengan menggunakan foto oranglain. Meskipun seseorang tampak bersahabat, mungkin sulit mengenali secara pasti siapa orang yang berbicara kepada Anda di internet. Beritahukan selalu kepada orangtua Anda atau seseorang yang Anda percayai ketika ada orang asing yang meminta menemui Anda secara pribadi agar pada akhirnya Anda tidak berada di dalam keadaan bahaya. Banyak pemangsa online menggunakan taktik cerdas untuk memikat Anda masuk ke keadaan bahaya, tetapi Anda bisa bersikap lebih cerdas. Ingatlah beragam resiko dan beragam petunjukini agar Anda bisa tetap selamat ketika Anda berbicara dengan oranglain di internet.

## Ciptakan kata sandi yang kokoh

2 menit

### Ciptakan kata sandi yang kokoh

Poin penting untuk tetap aman dan menjaga privasi informasi Anda di internet adalah dengan melinduni informasi Anda, akun Anda dan komputer Anda dengan menggunakan kata sandi yang kokoh.

**Saksikan video di bawah ini untuk mempelajari bagaimana menciptakan kata sandi yang efektif dan kokoh yang bisa melindungi informasi Anda.**

### [Video: Ciptakan kata sandi yang kokoh](https://www.microsoft.com/en-us/videoplayer/embed/RWtD0z)

Kata sandi menolong melindungi informasi dan akun pribadi Anda dari oranglain. Kata sandi itu penting sebagai gembok untuk pintu. Anda inginkan gembok yang kuat yang sulit dihancurkan dan akan mencegah masuknya orang-orang yang berbahaya. Anda juga tidak ingin siapapun menemukan kunci untuk gembok Anda. Kata sandi itu seperti gembok yang kokoh bagi akun Anda. Anda ingin kata sandi itu sulit ditebak oleh oranglain. Anda juga ingin agar kuncinya aman agar oranglain tidak bisa menemukannya. Ikutilah beberapa petunjuk ini untuk menciptakan kata sandi yang kokoh dan tetap aman.

Petunjuk nomor 1 (satu). Gunakan perpaduan antara huruf, angka, dan symbol di dalam kata sandi Anda. Gunakan perpaduan huruf besar, huruf kecil dan karakter, dan dengan menambahkan angka yang bisa meningkatkan kekuatan kata sandi Anda.

Petunjuk nomor 2 (dua). Hindari menggunakan kata-kata umum di kata sandi Anda. Ini termasuk kata-kata umum dan frase umum seperti password atau situs web dan kata kunci pribadi seperti ulang tahun Anda, nama Anda, atau kota kediaman Anda. Hacker bisa dengan mudah menebak frase ini di kata sandi Anda. Perpaduan unik antara karakter dna angka akan menciptakan kata sandi yang kokoh.

Petunjuk nomor 3 (tiga). Gunakan kata sandi lain untuk akun lainnya. Jika seseorang menebak kata sandi email Anda, keamanan dan privasi Anda bisa saja bermasalah jika Anda menggunakan kata sandi yang sama untuk akun bank. Gunakan kata sandi lain untuk akun online lainnya yang Anda miliki.

Petunjuk nomor 4 (empat). Kata sandi Anda itu hanya untuk Anda. Ketika Anda membagikannya ke oranglain, meskipun itu ke teman atau keluarga, maka lebih besar kemungkinannya oranglain akan menggunakan kata sandi Anda itu, atau tidak akan menjaga keamanannya. Simpan kata sandi Anda bagi diri Anda sendiri. Ketika Anda masuk (login) ke beragam akun, pastikan bahwa Anda keluar (logout) jika Anda sudah selesai, dan jangan menyimpan informasi login Anda di komputer publik.

Selain itu, hindari melakukan bisnis pribadi di komputer publik (komputer yang dipakai bergantian oleh lebih dari satu orang) karena ini akan memudahkan hacker untuk melihat informasi Anda. Ingatlah, gunakan kata sandi yang kokoh, dan mengamankan kata sandi itu penting untuk keamanan dan privasi Anda di internet. Ingatlah petunjuk-petunjuk ini ketika Anda menciptakan kata sandi baru, kata sandi yang kokoh.

## Jelaskan cara terbaik untuk membagikan informasi di internet

2 menit

### Cerdaslah ketika Anda berbagi

Ketika kita terhubung ke internet, kita mungkin sering melakukan banyak hal yang mengancam keamanan kita tanpa berpikir panjang tentang keamanan. Betapa pentingnya berpikir dua kali tentang apa yang Anda bagikan di internet dan ingatlah keamanan Anda.

**Saksikan video di bawah ini untuk mempelajari lebih lanjut tentang beragam resiko jika berbagi berlebihan di internet.**

### [Video: Berbagi berlebihan di internet](https://www.microsoft.com/en-us/videoplayer/embed/RWtSAV)

Internet dan web memungkinkan kita tetap terhubung ke teman-teman dna keluarga lintas negara. Kita bisa menggunakan media sosial dan aplikasi lain untuk melihat apa yang sedang terjadi di kehidupan teman-teman kita, berbagi berita pribadi, dan tetap terhubung satu sama lain, tetapi berbagi segala sesuatu di internet itu tidak selalu aman.

Pertimbangkan scenario ini. Harold mendapatkan mobil baru dan ingin agar teman-temannya melihatnya. Jadi, dia memposting fotonya ke media social. Mungkin ini sepertinya baik-baik saja, tetapi foto itu berisikan banyak informasi pribadi tentang Harold. Dari satu foto, siapapun bisa melihat nomor plat lisensi Harold, mobil jenis apa yang dia kemudikan, dan di mana dia tinggal.

Mungkin saja ini baik-baik saja bagi teman-temannya untuk melihatnya, tetapi bisa jadi berbahaya kalau salah orang yang menemukan informasi ini dan ingin menggunakannya dengan niat yang tidak baik. Betapa pentingnya mengingat keamanan dan privasi ketika Anda membagikan segala sesuatu di internet.

Ketika Anda mengatur profil di situs web media sosial, pastikan agar memeriksa pengaturan privasi akun Anda. Jika akun Anda disetel menjadi umum alias publik, maka siapapun bisa melihat informasi Anda dan apa yang Anda bagikan. Tetapi, gunakanlah pengaturan privasi di akun itu agar hanya koneksi pribadi Anda saja yang bisa melihat apa yang Anda bagikan.

Anda harus juga berhati-hati memilih ketika Anda menerima undangan untuk terhubung ke seseorang di media social. Sebagian besar aplikasi media sosial mempunyai cara untuk Anda menerima dan menolak permohonan, menerima seseorang menjadi teman Anda, atau pengikut Anda di situs itu. Setelah Anda menerima seseorang, orang itu mendapatkan akses langsung ke profil Anda dan segala sesuatu yang Anda bagikan. Ingatlah ini ketika Anda menerima permohonan, dan pastikan agar Anda hanya berinteraksi dengan orang yang Anda kenal dan percayai.

Bahkan ketika Anda mengendalikan siapa yang mendapatkan akses ke profil dan akun Anda, Anda tidak mengendalikan apa yang oranglain lakukan dengan informasi Anda. Ketika Anda membagikan sesuatu di internet, Anda tidak bisa menghapusnya. Jangan pernah membagikan di internet sesuatu yang Anda tidak ingin orang asing dan masyarakat umum melihatnya. Ingatlah selalu berpikir sebelum Anda membagikan. Ingatlah keamanan Anda, dan pilih dengan cermat ketika Anda membagikan segala sesuatu di internet.

### Coba Anda kerjakan sendiri

Apakah yang Anda pelajari dari video ini? Tuliskan 1-3 hal yang akan Anda ingat ketika Anda membagikan informasi pribadi Anda di internet.

## Jelaskan pentingnya mengatur jejak kaki digital

3 menit

### Jejak kaki digital Anda

Ada banyak hal yang bisa kita lakukan di internet, mulai dari browsing web, membagikan info terbaru di media sosial, sampai melakukan pembelian di internet. Anda harus ingat bahwa segala sesuatu yang Anda lakukan di internet menjadi bagian dari sejarah Anda atau jejak kaki digital (**digital footprint**) Anda di internet.

Anda harus memikirkan tentang jejak kaki digital Anda ketika Anda membagikan informasi atau melakukan hal-hal di internet karena hal-hal yang terjadi di internet itu sulit dihapus.

**Saksikan video di bawah ini untuk mempelajari jejak kaki digital Anda dan bagaimana mengaturnya.**

### [Video: Atur jejak kaki digital Anda](https://www.microsoft.com/en-us/videoplayer/embed/RWtV9U)

Jika Anda menggunakan internet, maka Anda harus menyadari jejak kaki digital Anda. Persis seperti jejak kaki fisik yang memperlihatkan kepada seseorang langkah-langkah di jalur kotoran, maka jejak kaki digital Anda merupakan sejarah seluruh kegiatan yang Anda lakukan di internet. Postingan media social apapun yang Anda lakukan, situs web apapun yang Anda kunjungi, dan informasi apapun yang Anda bagikan di internet akan memberikan sumbangsih terhadap jejak kaki digital Anda.

Setelah Anda memposting sesuatu di internet, postingan itu tidak bisa dihapus. Jadi, jejak kaki digital Anda bisa bertahan selamanya. Ini bisa merupakan hal baik jika jejak kaki digital Anda berisikan hal-hal yang memberikan reputasi baik kepada Anda di internet. Ini bisa menolong Anda membangun merek pribadi Anda. Sejarah Anda di internet bisa menolong aplikasi yang Anda gunakan untuk mengenal lebih jauh tentang Anda. Aplikasi itu bisa menggunakan informasi ini untuk melayani Anda dengan lebih baik lagi dengan menyesuaikan dengan hal-hal yang Anda sukai dan kebiasaan-kebiasaan harian Anda. Tetapi aplikasi itu bisa juga menggunakan informasi ini dengan cara yang tidak benar, dan membagikannya ke oranglain. Ingatlah beberapa petunjuk di bawah ini ketika Anda terhubung ke internet untuk mengatur jejak kaki digital Anda.

Petunjuk nomor 1 (satu). Kenali apa yang dikatakan oleh jejak kaki digital Anda tentang Anda. Oranglain menggunakan jejak kaki digital Anda untuk melakukan penilaian tentang Anda di internet. Ini bisa berisi bos ketika Anda melamar pekerjaan atau perekrut ketika Anda mengajukan permohonan program akademis. Betapa pentingnya mengetahui apa yang dikatakan oleh jejak kaki digital Anda tentang Anda dan bagaimana informasi Anda dipergunakan. Untuk melihat apa yang dikatakan oleh merek pribadi Anda di internet, Anda bisa mencarinya sendiri. Cari nama Anda di Bing search engine dan melihat hasil apa yang ditampilkan. Jika hasil ini tidak menunjukkan apa yang Anda inginkan, pikirkanlah apa yang Anda bagikan di internet dan informasi apa yang Anda izinkan dilihat oleh oranglain.

Petunjuk nomor 2 (dua). Aturlah pengaturan privasi Anda. Anda bisa memodifikasi pengaturan privasi di sebagian besar situs media social, dan beragam aplikasi online yang Anda gunakan. Ini bisa menolong Anda mengendalikan siapa yang melihat apa yang Anda bagikan, dan informasi apa yang tampil ketika seseorang mencari Anda di internet.

Petunjuk nomor 3 (tiga). Atur cookies Anda. Cookies merupakan catatan yang diberikan ke browser web Anda ketika Anda melakukan browsing di web. Cookies ini menolong aplikasi menelusuri informasi yang dibutuhkan ketika Anda sedang menggunakan aplikasi itu. Ini bisa menolong aplikasinya agar bekerja lebih baik lagi untuk Anda. Tetapi, data ini juga memberikan sumbangsih terhadap jejak kaki digital Anda. Anda bisa menggunakan pengaturan di browser Anda untuk membatasi atau memblokir penggunaan cookies di situs web tertentu.

Petunjuk nomor 4 (empat). Pikirkan sebelum Anda membagikan. Setelah Anda membagikan sesuatu di internet, maka Anda tidak bisa menariknya kembali. Pastikan bahwa Anda baik-baik saja dengan sesuatu yang menjadi bagiandari jejak kaki digital Anda di hadapan publik sebelum Anda membagikannya. Jejak kaki digital Anda bisa hidup selamanya. Ingatlah petunjuk-petunjuk ini demi memastikan bahwa Anda senang dengan jejak kaki digital Anda dan bagaimana jejak kaki digital Anda itu dipergunakan.

Uji Pengetahuan

3 menit

1. Manakah di antara komponen-komponen di bawah ini yang harus Anda cari di URL dari halaman web untuk memastikan bahwa Anda berada di situs web yang aman?

* http
* secure
* **https - Benar! "https" berarti halaman web-nya itu aman.**
* ssh

1. Manakah di antara kata sandi ini yang terkokoh?

* **John@453 - Benar! Kata sandi ini berisikan huruf besar, huruf kecil, karakter khusus dan angka.**
* john500
* JoHn300
* 125893

1. Jejak kaki digital Anda adalah:

* Ukuran informasi di akun online Anda.
* Jumlah orang yang terhubung dengan Anda di internet.
* **Catatan tentang segala sesuatu yang Anda kerjakan dan ucapkan di internet. - Benar! Jejak kaki digital Anda memudahkannya untuk menelusuri kegiatan-kegiatan Anda di internet.**
* Nama pengguna yang Anda gunakan di internet.
* r using strong passwords.

## Ringkasan

1 menit

Selamat!

Anda sudah menyelesaikan modul keamanan dan privasi di internet, dan sekarang bisa menjawab sendiri pertanyaan-pertanyaan di bawah ini:

1. Apa sajakah bahaya menggunakan internet dan web?
2. Apa sajakah tanda-tanda resiko keamanan dan penipuan di internet?
3. Langkah apakah yang bisa Anda ambil agar tetap aman ketika menggunakan internet?
4. Bagaimanakah caranya Anda mengatur jejak kaki digital Anda?

**the following video to learn how to create strong, effective passwords that**

# Kesopanan di internet

9 menit | 5 unit

Di modul ini, Anda akan belajar lebih lanjut tentang hak-hak dan cara-cara terbaik untuk menggunakan informasi di internet. Anda juga akan belajar tentang cyberbullying (intimidasi melalui internet atau intimidasi online).

Pengenalan

1 menit

Kita bisa menggunakan internet untuk mengakses banyak informasi dan berkomunikasi dengan oranglain, tetapi kita harus memastikan agar kita bersikap sebagai warga digital yang bertanggungjawab.

Di pelajaran ini, Anda akan belajar bagaimana menggunakan internet dan web dengan sikap yang bertanggungjawab.

**Di akhir pelajaran ini, Anda akan bisa:**

1. Jelaskan hak-hak yang dimiliki oleh setiap orang terhadap informasi dan konten yang dibagikan di web.
2. Jelaskan cara-cara terbaik untuk menggunakan informasi yang ditemukan di web.
3. Jelaskan dampak dari perlakuan buruk terhadap oranglain di web.
4. **protect your information.**

## Jelaskan cara terbaik untuk menggunakan informasi yang ditemukan di web

2 menit

### Gunakan informasi dengan rasa tanggungjawab

Meskipun mudah untuk mengakses informasi di dunia digital, tetapi ada beberapa aturan untuk diingat di saat Anda ingin menggunakan informasi yang Anda temukan di internet.

**Saksikan video di bawah ini untuk mempelajari beberapa pedoman untuk menggunakan informasi yang Anda temukan di internet.**

### Video: Gunakan informasi dengan rasa tanggungjawab

Internet menyediakan informasi dan beragam kemungkinan tanpa batas. Kita bisa menemukan apapun dari video lucu, sampai lagu-lagu favorit, atau informasi tentang cara menyelesaikan permasalahan pekerjaan rumahan, tetapi kita harus bertanggungjawab terhadap informasi yang kita temukan di internet.

Mempertimbangkan scenario. [Harold ingin menulis buku masakan, dan menjualnya di internet. Dia tidak pandai memotret sehingga dia mencari foto-foto di internet. Dia mendownload foto-foto di makanan-makanan lain, dan memasukkan](file:///C:\Users\v-cimc\Desktop\APS\Participate%20safely%20and%20responsibly%20online110819\SCO1\Launch.htm) foto-foto itu ke dalam bukunya. Mungkin, tampaknya ini boleh-boleh saja karena mudah dilakukan, tetapi ini bukanlah cara yang adil dan bertanggungjawab di dalam menggunakan informasi yang ditemukan di internet.

Di saat seseorang meletakkan karya asli miliknya di internet termasuk kata-kata, video, musik, dan lainnya, maka orang itu menjadi pemilik dari konten itu. Sebagai pemilik, orang itu memiliki hak-hak tertentu yang biasanya dianggap sebagai hak cipta untuk memutuskan bagaimana konten itu bisa digunakan. Jika Anda menggunakan kata-kata atau karya oranglain sebagai milik Anda, maka dianggap penjiplakan. Ini tidak adil bagi penulis aslinya dan bisa mendatangkan mendatangkan masalah ke Anda. Jika Anda ingin menggunakan konten milik oranglain di dalam karya Anda, pastikan bahwa Anda menyebutkan orang itu untuk memberikan penghargaan terhadap karyanya.

Di saat Anda sedang menggunakan karya milik oranglain di produk yang sedang Anda jual, Anda harus pertama-tama mendapatkan izin dari penulisnya. Mungkin Anda juga harus membayar lisensi untuk menggunakan karya oranglain. Terkadang, penulis konten itu menyediakan karyanya untuk dipakai gratis.

Anda bisa menggunakan search engine (alias mesin pencari) seperti Bing untuk menemukan foto-foto, media, dan konten jenis lain yang tersedia untuk dipakai oleh oranglain. Di saat Anda menggunakan internet dan mencari informasi di internet, pastikan bahwa Anda menggunakannya dengan adil dan bertanggungjawab.

## Jelaskan dampak dari perlakuan buruk terhadap oranglain di web

3 menit

### Intimidasi melalui Internet (Cyberbullying)

Internet memungkinkan kita terhubung ke oranglain dari seluruh dunia. Sayangnya, orang tidak selalu memberikan perlakuan baik terhadap oranglain di internet.

**Intimidasi Online (Cyberbullying)** merupakan jenis intimidasi yang terjadi di internet. Bisa saja dengan mudah mengirimkan pesan yang tidak baik, atau menyebarkan isu-isu buruk tentang oranglain, tetapi ini bisa berbahaya bagi orang yang dituju.

**Saksikan video di bawah ini untuk mempelajari petunjuk-petunjuk untuk mencegah intimidasi online dan petunjuk-petunjuk bagaimana menjadi warga digital.**

### [Video: Perlakukan oranglain di internet dengan rasa hormat](https://www.microsoft.com/en-us/videoplayer/embed/RWtVa9)

Internet dan aplikasi media sosial

Internet dan aplikasi media social menghubungkan kita ke teman-teman, keluarga, dan teman sebaya dengan cara baru. Terkadang, orang mengambil keuntungan dari aplikasi-aplikasi seperti ini, dan memanfaatkannya untuk menyebarkan pesan negatif tentang oranglain.

Intimidasi online (alias [Cyberbullying, atau intimidasi yang terjadi di internet)](file:///C:\Users\v-cimc\Desktop\APS\Participate%20safely%20and%20responsibly%20online110819\SCO1\Launch.htm) bisa saja seburuk intimidasi di dunia nyata. Orang bisa menggunakan internet untuk mengirimkan pesan yang tidak baik, menyebarkan isu-isu palsu, atau membagikan informasi pribadi oranglain tanpa izin. Di saat seseorang mengalami intimidasi online alias cyberbully, perasaan orang itu bisa terluka, dan nama baik (alias reputasi) orang itu bisa rusak. Anda tidak bisa selalu menghindari intimidasi online (alias cyberbully), tetapi Anda bisa berperanserta menjadikan internet itu lebih ramah dan lebih aman untuk setiap orang.

Ini merupakan beberapa pedoman yang bisa Anda ikuti untuk meningkatkan digital civility (alias kesopanan di dunia digital) di internet:

* Jalani kehidupan sesuai Golden Rule (alias Kaidah Kencana) yang artinya Perlakukanlah oranglain seperti Anda ingin diri Anda diperlakukan[, entah itu di dunia nyata maupun di internet](file:///C:\\Users\\v-cimc\\Desktop\\APS\\Participate%20safely%20and%20responsibly%20online110819\\SCO1\\Launch.htm).
* Hindari tindakan mengirim pesan yang tidak baik, dan hindari peranserta di dalam sikap yang bisa melukai perasaan oranglain.
* Hormati perbedaan. Kita semua berbeda-beda dalam banyak hal. Di saat Anda berinteraksi dengan oranglain di internet, hormati perbedaan pendapat, pengalaman dan budaya orang itu. Bahkan kalaupun Anda tidak setuju dengan sesuatu yang orang orang itu bagikan di internet, Anda harus tetap memperlakukan orang lain itu dengan rasa hormat, dan menjadikan internet itu sebagai tempat yang ramah untuk berkomunikasi.
* Berhentilah sejenak sebelum menjawab. Sebelum Anda membagikan apapun itu di internet, selalu berhentilah sejenak dan pikirkan dampaknya. Apakah pesan Anda itu akan melukai perasaan oranglain? Apakah pesan Anda itu akan merusak nama baik Anda, atau merusak keamanan atau nama baik oranglain?
* Berpikirlah dua kali sebelum membagikannya di internet. Ambil sikap positif untuk diri Anda dan oranglain. Jika Anda merasa tidak aman di internet, maka Anda harus merasa nyaman menarik diri Anda sendiri dari keadaan itu, dan melaporkannya ke oranglain yang Anda percayai.
* Di saat Anda melihat tindakan kejam atau berbahaya di internet, tawarkanlah dukungan ke orang yang terlibat, dan laporkan kejadian itu ke seseorang yang Anda percayai. Kita semua bisa berperanserta menjadikan internet itu sebagai tempat yang aman dan ramah untuk setiap orang.
* Berperansertalah, dan jadilah warga digital yang bertanggungjawab di internet.

## Uji Pengetahuan

2 menit

1. Manakah di antara tindakan-tindakan ini yang tidak melanggar hak cipta?

* Menggunakan foto seseorang di buku yang Anda terbitkan tanpa izin dari orang itu.
* **Mengutip paragraf dari buku seseorang dan menyebutkan orang itu - Benar! Anda menghormati hak cipta di saat menyebutkan pemiliknya.**
* Menjual video seseorang dengan memakai nama Anda.
* Menjual buku seseorang tanpa lisensi (alias surat izin).

1. Intimidasi online (Cyberbullying) bisa terjadi:

* Hanya di aplikasi media sosial.
* Hanya melalui email.
* Hanya di SMS.
* **Di aplikasi sosial media dan SMS, dan melalui email. - Benar! Cyberbullying bisa terjadi di dalam komunikasi online, apapun jenisnya.**

## Ringkasan

1 menit

Selamat!

Anda sudah menyelesaikan modul Kesopanan di internet, dan sekarang Anda bisa menjawab sendiri pertanyaan-pertanyaan di bawah ini:

1. Apakah yang harus Anda lakukan di saat Anda ingin menggunakan informasi yang Anda temukan di internet?
2. Apakah yang bisa Anda lakukan untuk mencegah atau mengakhiri intimidasi online (alias cyberbullying)?

# Cetak sertifikat Anda

2 menit | 2 unit

Anda harus menyelesaikan semua modul di kursus ini agar Anda bisa menerima sertifikat Anda.

## Terimalah kreditnya

1 minute

### Selesai

Selamat atas selesainya modul Berpartisipasilah secara online dengan aman dan bertanggungjawab. Pilih **Receive credit** (Terimalah kreditnya) untuk menyelesaikan kursus ini, dan menerima sertifikat Anda.

### Kreditnya Diterima

Selamat atas selesainya modul Berpartisipasilah secara online dengan aman dan bertanggungjawab.

Di kotak di bawah ini, silahkan ketikkan nama Anda seperti apa Anda ingin nama Anda itu muncul di sertifikat Anda. Kemudian, pilih **View certificate** (Tampilkan sertifikat).