Participe on-line com segurança e responsabilidade

26 minutos

Neste caminho de aprendizagem, você será introduzido aos riscos de segurança que você pode enfrentar ao usar a internet. Você vai aprender sobre golpes on-line e como evitá-los. Você também aprenderá sobre as melhores práticas para compartilhar informações on-line. Além disso, você será apresentado ao cyberbullying.

# Segurança e privacidade on-line

17 minutos | 8 unidades

Neste módulo, você aprenderá sobre alguns dos riscos de segurança que podem afetá-lo quando você está usando o Internet, e pontas para permanecer seguro e manter sua informação confidencial em linha.

## Proteja-se do phishing

3 minutos

### Proteja-se do phishing

Embora existam muitas coisas positivas que podemos fazer on-line, devemos estar sempre cientes dos riscos de segurança. Há muitos golpes que os predadores on-line usam para acessar as informações das pessoas on-line.

Você deve estar ciente desses golpes para que você possa fazer o seu melhor para evitá-los. **Phishing**  é um golpe on-line comum que você deve estar ciente.

**Assista ao vídeo a seguir para saber mais sobre phishing e como se proteger desse golpe on-line.**

### Vídeo: Proteja-se do phishing

A Internet nos oferece muitas possibilidades. Podemos falar com outras pessoas, fazer compras online e fazer negócios pessoais, tudo em um só lugar. Mas essas interações online nem sempre são seguras. Vamos falar sobre um golpe online popular do qual você deve estar ciente. Uma maneira comum de fisgar um peixe é colocar comida em um anzol para que o peixe queira comê-la. Quando ele morde a comida, é fisgado. Os golpes de phishing na Internet funcionam da mesma maneira. Pessoas que querem roubar suas informações são como pescadores. Elas enviam um email ou mensagem instantânea por meio de um site de mídia social ou um jogo online. Muitas vezes fingem ser alguém que não são e lhe pedem informações privadas ou pedem que você clique em um hiperlink, para que você possa concluir uma tarefa importante. Se você lhes der as informações ou clicar no hiperlink, será fisgado. Mas não se preocupe. Estas quatro práticas podem ajudar a protegê-lo contra golpes de phishing. Prática número um: tenha cuidado com mensagens suspeitas. Os golpistas tentam fazer suas mensagens parecerem Pense duas vezes quando receber uma mensagem suspeita e evite compartilhar informações pessoais por mensagens ou emails. Isso inclui seu endereço residencial, informações bancárias, senhas e muito mais. Não clique em um link nem baixe um arquivo se você não conhece ou não confia no remetente. Prática número dois: procure sinais de que uma página da Web é segura e está protegida. Antes de fornecer informações de cartão de crédito, digitar uma senha ou fornecer outras informações pessoais, verifique se você está em um site seguro e confiável. A maioria dos sites seguros tem o prefixo https no início da URL na barra de endereços do navegador. Além disso, verifique se você está na página certa. Os golpistas muitas vezes tentam levar você para páginas da Web que parecem ser oficiais e usam erros ortográficos em nomes da empresas para enganá-lo. www.microsoft.net não é o mesmo que o site oficial da Microsoft em www.microsoft.com. Verifique sempre a URL para garantir que está na página certa. Prática número três: mantenha seu navegador da Web e seu sistema operacional atualizados. Você pode ativar as atualizações automáticas para garantir que as últimas versões do software sejam instaladas automaticamente em seu computador. Manter o software do dispositivo atualizado significa que você vai receber o últimas atualizações de segurança que ajudam a proteger seu computador. Prática número quatro: instale software antimalware confiável em seus dispositivos. Esse é um software especial projetado para proteger seu computador contra hackers e software perigoso. Não seja o próximo peixe a ser fisgado. Ao usar a Internet, lembre-se de pensar antes de clicar, baixar ou compartilhar para se proteger contra golpes de phishing online.

## Comunicar-se com segurança on-line

2 minutos

### Comunicar-se com segurança on-line

A internet nos permite comunicar com outras pessoas de novas maneiras. No entanto, nem sempre é seguro se comunicar com outras pessoas on-line. Você nem sempre sabe ao certo com quem você está falando quando você está na internet, então você tem que ter cuidado para ficar seguro.

**Assista ao vídeo a seguir para saber como se comunicar com segurança on-line.**

### Vídeo: Comunicar com segurança on-line

Usando a Internet, podemos nos comunicar com outras pessoas em todo o mundo de novas maneiras. Isso tem muitos benefícios, mas também há alguns perigos. Há predadores online que usam a Internet todos os dias. Esses predadores muitas vezes fingem ser pessoas que não são. Assim, pode ser difícil saber com quem você está falando online. Aqui estão três dicas que você pode usar para se manter seguro contra predadores ao se comunicar online. Dica número um: confie em seus instintos. Se alguém deixa você nervoso ou desconfortável, pare de se comunicar com ele e conte imediatamente a alguém em que você confia. A maioria dos sites e sites de mídia social tem ferramentas que você pode usar para relatar atividades suspeitas. Dica número dois: limite o que você compartilha. Os predadores online muitas vezes tentam fazer você compartilhar suas informações pessoais por meio de emails e mensagens. Evite compartilhar informações pessoais com estranhos online. Dica número três: mantenha distância. Pense duas vezes antes de se encontrar em pessoa com alguém com quem você só conversou online. Os predadores online muitas vezes usam a mídia social para fingir ser alguém diferente, configurando perfis falsos com fotos de outras pessoas. Mesmo que alguém pareça amigável, pode ser difícil saber com certeza com quem você está falando online. Sempre diga a um responsável ou a alguém em quem você confia quando um estranho online pedir para conhecê-lo pessoalmente, para que você não acabe em uma situação perigosa. Muitos predadores online usam táticas inteligentes para atraí-lo para situações perigosas, mas você pode ser mais inteligente. Lembre-se desses riscos e dicas, para que você possa ficar seguro quando falar com as pessoas online.

## Criar senhas fortes

2 minutos

### Criar senhas fortes

Uma grande parte de se manter seguro e manter suas informações privadas on-line é proteger suas informações, suas contas e seu computador usando senhas fortes.

**Assista ao vídeo a seguir para saber como criar senhas fortes e eficazes que possam proteger suas informações.**

### Vídeo: Criar senhas fortes

As senhas ajudam a proteger suas informações pessoais e as contas contra outras pessoas. Uma senha é tão importante quanto a fechadura de uma porta. Você quer ter uma fechadura forte que seja difícil de quebrar e impeça que pessoas perigosas entrem. Você também não quer que ninguém encontre as chaves de seu cadeado. Uma senha forte é como uma fechadura forte para sua conta. Você quer que seja difícil que outras pessoas a adivinhem. Também quer que ela seja segura e protegida, para que os outros não possam encontrá-la. Siga essas dicas para criar senhas fortes e mantê-las seguras. Dica número um: use uma combinação de letras, números e símbolos em sua senha. Usar uma combinação de letras maiúsculas e minúsculas e caracteres e números adicionais pode aumentar a força de sua senha. Dica número dois: evite usar palavras comuns na senha. Isso inclui palavras comuns e frases como senha ou site, bem como palavras-chave pessoais, como seu aniversário, nome ou cidade natal. Os hackers podem facilmente adivinhar essas frases em sua senha. Uma combinação exclusiva de caracteres e números cria uma senha mais forte. Dica número três: use senhas diferentes para contas diferentes. Se alguém adivinhar sua senha de email, sua segurança e privacidade poderão ser prejudicadas se você usar a mesma senha para sua conta bancária. Em vez disso, use senhas diferentes para cada conta online que você tem. Dica número quatro: sua senha serve apenas para você. Quando você a compartilha com outros até mesmo os amigos e a família, é mais provável que alguém mais a utilize ou não a mantenha segura. Guarde suas senhas para si mesmo. Quando você fizer logon em contas, não se esqueça de sair quando terminar e não salve suas informações de logon em um computador público. Além disso, evite fazer negócios pessoais em computadores e redes públicas, pois isso torna mais fácil para os hackers acessar suas informações. Lembre-se, usar senhas fortes e mantê-las seguras é importante para sua segurança online e privacidade. Lembre-se dessas dicas ao criar uma nova senha.

## Descreva as melhores práticas para compartilhar informações on-line

2 minutos

### Seja inteligente quando compartilhar

Quando vamos em linha, muitas vezes podemos fazer muitas coisas que ameaçam a nossa segurança sem pensar muito sobre isso. É importante pensar duas vezes sobre o que você compartilha on-line e manter sua segurança em mente.

**Assista ao vídeo a seguir para saber mais sobre os riscos de compartilhar demais on-line.**

### Vídeo: Oversharing online

Com a Internet e a Web, podemos permanecer conectados com os amigos e a família em todo o mundo. Podemos usar a mídia social e outras plataformas para ver o que está acontecendo nas vidas dos amigos, compartilhar notícias pessoais e manter contato com outras pessoas, mas compartilhar itens online nem sempre é seguro. Considere este cenário: Harold adquire um carro novo e quer que os amigos o vejam. Então, ele posta uma foto do carro nas redes sociais. Pode parecer uma boa ideia, mas a imagem inclui muitas informações pessoais de Harold. Qualquer um pode ver o número da placa dele, que tipo de carro ele dirige e onde ele mora, com apenas uma foto. Pode não ser problema que seus amigos vejam isso, mas poderá ser perigoso se a pessoa errada encontrar essas informações e quiser usá-las de forma indevida. É importante manter a segurança e a privacidade quando você compartilha itens online. Ao configurar perfis em sites de mídia social, confira as configurações de privacidade de sua conta. Se sua conta for definida como pública, qualquer um poderá ver suas informações e o que você compartilha. Em vez disso, use a configuração privada nas contas, para que apenas suas conexões pessoais possam ver o que você compartilha. Você também deve ser seletivo ao aceitar convites para se conectar com alguém na mídia social. A maioria das plataformas de mídia social tem uma maneira de aceitar e negar pedidos para que alguém seja seu amigo ou seguidor no site. Quando você aceita alguém, essa pessoa tem acesso direto a seu perfil e aos itens que você compartilha. Lembre-se disso ao receber uma solicitação e só interaja com pessoas que você conhece e em quem confia. Mesmo quando você controla quem tem acesso a seus perfis e contas, não pode controlar o que outras pessoas fazem com suas informações. Quando você compartilha algo online, não pode apagá-lo. Nunca compartilhe algo online que você não quer que estranhos e o público vejam. Lembre-se sempre de pensar antes de compartilhar. Cuide de sua segurança e faça escolhas inteligentes ao compartilhar itens online.

### Experimente você mesmo

O que você aprendeu com este vídeo? Anote 1-3 coisas que você terá em mente quando você compartilhar informações pessoais on-line.

## Descreva a importância de gerenciar sua pegada digital

3 minutos

### Sua pegada digital

Há muito que podemos fazer on-line, de navegar na web, para compartilhar atualizações nas mídias sociais, para fazer compras on-line. Você deve ter em mente que tudo o que você faz on-line torna-se parte de seu histórico on-line, ou sua **pegada digital**.

Você deve pensar sobre sua pegada digital quando você compartilha informações ou fazer coisas on-line, porque as coisas que acontecem on-line são difíceis de apagar.

**Assista ao vídeo a seguir para saber mais sobre sua pegada digital e como gerenciá-la.**

### Vídeo: Gerenciar sua pegada digital

Se você usa a Internet, deve estar ciente de sua pegada digital. Assim como as pegadas físicas que mostram a alguém os passos em um caminho de terra, sua pegada digital é um histórico de toda a atividade que você realiza online. As postagens que você cria nas redes sociais, os sites que você visita e qualquer informação que você compartilha online contribuem para sua pegada digital. Quando você posta algo online, isso não pode ser apagado. Então, sua pegada digital pode durar para sempre. Pode ser algo bom se sua pegada digital inclui itens que lhe dão uma reputação positiva online. Isso pode ajudá-lo a construir sua marca pessoal. Seu histórico online também pode ajudar os aplicativos que você usa a saber mais sobre você. Eles podem usar essas informações para servi-lo melhor se ajustando aos itens de que você gosta e seus hábitos diários. Mas eles também podem usar essas informações de maneira indevida e compartilhá-las com outras pessoas. Lembre-se das dicas a seguir ao ficar online para gerenciar sua pegada digital. Dica número um: saiba o que sua pegada diz sobre você. Outras pessoas usam sua pegada digital para fazer julgamentos sobre você online. Isso pode incluir empregadores, quando você se candidata a um emprego, ou recrutadores, quando você se candidata a programas acadêmicos. É importante saber o que sua pegada digital diz sobre você e como suas informações estão sendo usadas. Para saber qual é a sua marca pessoal online, você pode procurar por si mesmo. Pesquise seu nome no mecanismo de pesquisa Bing e veja quais resultados são exibidos. Se esses resultados não mostram o que você quer, reflita sobre o que você compartilhar online e que informações você permite que outras pessoas vejam. Dica número dois: gerencie suas configurações de privacidade. Você pode modificar as configurações de privacidade da maioria dos sites de mídia social e aplicativos online que usa. Isso pode ajudá-lo a controlar quem vê o que você compartilha e que informações são mostradas quando alguém procura por você online. Dica número três: gerencie seus cookies. Os cookies são notas fornecidas a seu navegador enquanto você navega pela Web. Esses cookies ajudam os aplicativos rastrear informações de que eles precisa enquanto você os utiliza. Isso pode ajudar o aplicativo a funcionar melhor para você. Mas esses dados também contribuem para sua pegada digital. Você pode usar as configurações do navegador para limitar ou bloquear o uso de cookies em determinados sites. Dica número quatro: pense antes de compartilhar. Quando você compartilha algo online, não pode apagá-lo. Tenha certeza de que você aceita que algo faça parte de sua pegada digital pública antes de compartilhar esse item. Sua pegada digital pode viver para sempre. Lembre-se dessas dicas para ter certeza de que você está satisfeito com sua pegada digital e como ela é usada.

Verificação de conhecimento

3 minutos

1. Qual dos seguintes componentes você deve procurar na URL de uma página web, para se certificar de que você está em um site seguro?

* http http
* Seguro
* **https - Correto! "https" significa que a página da Web está segura.**
* Ssh

1. Qual dessas senhas é a mais forte?

* **John@453 - Correto! Esta senha contém carácter e números maiúsculas, minúsculas, especiais.**
* john500 John500
* John300 John300
* 125893

1. Sua pegada digital é:

* O tamanho das informações em suas contas on-line.
* O número de pessoas com as pessoas com as pessoas que você está conectado on-line.
* **Um registro de tudo o que você faz e diz on-line. Correto! Sua pegada digital facilita o controle de suas ações on-line.**
* Seu nome de usuário on-line.
* r usando senhas fortes.

## Resumo

1 minuto

Parabéns!

Você completou o módulo de segurança e privacidade on-line e agora pode responder às seguintes perguntas por conta própria:

1. Quais são alguns perigos de usar a internet e a web?
2. Quais são alguns sinais de riscos de segurança e golpes on-line?
3. Que medidas você pode tomar para ficar seguro ao usar a internet?
4. Como você pode gerenciar sua pegada digital?

**o vídeo a seguir para aprender a criar senhas fortes e eficazes que**

# Civilidade on-line

9 minutos | 5 unidades

Neste módulo, você aprenderá mais sobre direitos e melhores práticas para o uso de informações on-line. Você também vai aprender sobre cyberbullying.

Introdução

1 minuto

Podemos usar a internet para acessar muitas informações e nos comunicar com outras pessoas, mas temos que ter certeza de que estamos nos comportando como cidadãos digitais responsáveis.

Nesta lição, você vai aprender a usar responsavelmente a internet e a web.

**Até o final desta lição você será capaz de:**

1. Descreva os direitos que as pessoas têm de informações e conteúdo compartilhado na web.
2. Descreva as melhores práticas para o uso de informações encontradas na web.
3. Descreva as implicações de tratar os outros mal na web.
4. **proteger suas informações.**

## Descreva as melhores práticas para o uso de informações encontradas na web

2 minutos

### Use as informações de forma responsável

Embora o acesso à informação seja fácil no mundo digital, existem algumas regras a ter em mente quando você deseja usar informações que você encontra on-line.

**Assista ao vídeo a seguir para saber algumas das diretrizes para o uso de informações que você encontra on-line.**

### Vídeo: Use as informações de forma responsável

A Internet nos dá informações e possibilidades ilimitadas. Podemos encontrar qualquer coisa, desde vídeos engraçados até nossas músicas favoritas ou informações sobre como resolver um problema da lição de casa, mas devemos ser responsáveis com as informações que encontramos online. Considere este cenário. Harold quer escrever um livro de receitas e vendê-lo online. Ele não sabe tirar boas fotos, então pesquisa imagens online. Ele baixa imagens de diferentes alimentos e as inclui em seu livro. Pode parecer uma boa ideia, pois é algo fácil de fazer, mas não é uma maneira justa ou responsável de usar informações encontradas online. Quando alguém coloca seu trabalho original online, incluindo suas palavras, imagens, vídeos, música e muito mais, se torna o proprietário do conteúdo. Como proprietário, ele tem certos direitos, geralmente considerado direitos autorais, para decidir como esse conteúdo pode ser usado. Se você usar as palavras ou o trabalho de outra pessoa como se fosse seu, isso será considerado plágio. Isso não é justo para o autor original e pode colocar você em apuros. Se você quiser usar o conteúdo de outra pessoa em seu trabalho, não deixe de fazer referência a essa pessoa para lhe dar crédito referente a seu trabalho. Quando você usa trabalho de alguém em um produto que você está vendendo, primeiro deve obter a permissão do autor. Você também pode ter que pagar por uma licença para usar o trabalho de alguém. Às vezes, os autores de conteúdo disponibilizam seu trabalho para uso gratuito. Você pode usar mecanismos de pesquisa como o Bing para encontrar imagens, mídia e outros tipos de conteúdo que estão disponíveis para uso por outras pessoas. Ao usar a Internet e encontrar informações online, não deixe de usá-las de forma justa e responsável.

## Descreva as implicações de tratar os outros mal na web

3 minutos

### Cyberbullying

A internet nos permite nos conectar com outras pessoas on-line de todo o mundo. Infelizmente, as pessoas nem sempre tratam uns aos outros muito bem online.

**Cyberbullying** é um tipo de bullying que ocorre ainternet. Pode ser fácil enviar mensagens médias ou espalhar rumores negativos sobre outras pessoas, mas isso pode ser perigoso para a pessoa que é alvo.

**Assista ao vídeo a seguir para aprender dicas para prevenir o cyberbullying e ser um cidadão digital.**

### Vídeo: Trate os outros respeitosamente on-line

### A Internet e as plataformas de mídia social nos conectam com os amigos, a família e os colegas de novas maneiras. Às vezes, as pessoas tiram vantagem dessas plataformas e as usam para espalhar mensagens negativas sobre os outros.

### 

### O cyberbullying, ou o bullying que acontece na Internet, pode ser tão ruim quanto o bullying que ocorre pessoalmente. As pessoas podem usar a Internet para enviar mensagens maldosas a alguém, espalhar boatos ou compartilhar informações privadas de alguém sem permissão. Quando uma pessoa é vítima de cyberbullying, pode ser magoada e sua reputação pode ser prejudicada. Você nem sempre pode impedir o cyberbullying, mas pode desempenhar um papel para tornar a Internet mais amigável e segura para todos.

### Aqui estão algumas diretrizes que você pode seguir para promover a civilidade digital online:

* Siga a Regra de Ouro. Trate os outros do jeito que você quer ser tratado, em pessoa ou online.
* Evite enviar mensagens negativas e participar de algum comportamento que possa machucar outra pessoa.
* Respeite as diferenças. Somos todos diferentes em muitos aspectos. Ao interagir com as pessoas online, respeite suas diferenças de opinião, experiência e cultura. Mesmo que você não concorde com algo que outra pessoa compartilha online, ainda deve tratá-la com respeito e tornar a Internet um espaço amigável para a comunicação.
* Pare antes de responder. Antes de compartilhar algo online, sempre faça uma pausa e reflita sobre as consequências. Sua mensagem magoará outra pessoa? Isso prejudicará sua reputação ou a segurança ou a reputação de outras pessoas?
* Pense duas vezes antes de compartilhar online. Defenda a si mesmo e aos outros. Se você se sentir inseguro online, deverá se sentir à vontade para se afastar de uma situação e relatá-la a alguém em quem você confie.
* Quando você presenciar atividade cruel ou perigosa online, ofereça apoio aos envolvidos e relate o incidente a alguém em quem confie. Todos nós podemos desempenhar um papel para tornar a Internet um lugar seguro e amigável para todos.
* Faça sua parte e seja um cidadão digital responsável online.

## Verificação de conhecimento

2 minutos

1. Qual dessas ações não está violando direitos autorais?

* Usando as imagens de alguém em um livro que você publica sem a sua permissão.
* **Citando um parágrafo do livro de alguém e referenciando-os - Correto! Você observa os direitos autorais quando cita o proprietário.**
* Vender o vídeo de alguém em seunome.
* Vender o livro de alguém semlicença.

1. O cyberbullying pode ocorrer:

* Apenas em plataformas de mídia social.
* Apenas através de e-mails.
* Apenas em SMS.
* **Em plataformas de mídia social e SMS, e através de e-mails. Correto! Cyberbullying pode ocorrer em qualquer tipo de comunicação on-line.**

## Resumo

1 minuto

Parabéns!

Você completou o módulo de civilidade on-line e agora pode responder às seguintes perguntas por conta própria:

1. O que você deve fazer quando você quer usar informações que você encontra on-line?
2. O que você pode fazer para prevenir ou acabar com o cyberbullying?

# Imprima o seu certificado

2 minutos | 2 unidades

Você deve completar todos os módulos neste curso para receber o seu certificado.

## Receber crédito

1 minuto

### Completa

Parabéns pela conclusão participar com segurança e responsabilidade on-line. Selecione **receber crédito** para concluir o curso e receber seu certificado.

### Crédito recebido

Parabéns pela conclusão participar com segurança e responsabilidade on-line.

Na caixa abaixo, por favor, digite seu nome como você gostaria que ele apareça em seu certificado, em seguida, selecione **certificado view**.