Participe de forma segura e responsável online

26 minutos

Neste caminho de aprendizagem, você será introduzido para os riscos de segurança que você pode enfrentar durante a utilização da internet. Você vai aprender sobre fraudes online e como evitá-los. Você também vai aprender sobre as melhores práticas para partilhar informações on-line. Além disso, será introduzido no ciberbullying.

# Segurança e privacidade on-line

17 minutos ! 8 unidades

Neste módulo, você vai aprender sobre alguns dos riscos de segurança que podem afetá-lo quando você está usando a internet, e dicas para se manter seguro e manter a sua informação privada on-line.

## Proteja-se do phishing

3 minutos

### Proteja-se do phishing

Embora haja muitas coisas positivas que podemos fazer online, devemos estar sempre cientes dos riscos para a segurança. Há muitos esquemas que os predadores online usam para aceder à informação das pessoas online.

Deve estar ciente destes esquemas para que possa fazer o seu melhor para evitá-los. **Phishing**  é um esquema online comum que deves estar a par.

**Veja o seguinte vídeo para saber mais sobre phishing e como se proteger deste esquema online.**

### Vídeo: Proteja-se do phishing

A Internet oferece-nos muitas possibilidades. Podemos falar com outras pessoas, fazer compras online e fazer negócios, tudo no mesmo lugar. Mas nem sempre estas interações online são seguras. Vamos falar sobre um popular esquema online de que deverá estar ciente. Uma forma comum de pescar um peixe é colocar isco num anzol, porque o peixe vai querer comê-lo. Assim que mordam o isco, ficarão presos no anzol. Os esquemas de phishing na Internet funcionam da mesma forma. As pessoas que querem roubar as suas informações são como os pescadores. Enviam-lhe um e-mail ou uma mensagem instantânea através de um site de redes sociais ou de um jogo online. Muitas vezes fingem ser alguém que não são e pedem-lhe informações privadas ou dizem-lhe para clicar numa hiperligação para que possa executar uma tarefa importante. Se lhes fornecer as informações ou clicar na hiperligação, estará a morder o isco. Mas não se preocupe. Estas quatro práticas podem ajudar a protegê-lo contra esquemas de phishing. Prática número um: tenha cuidado com mensagens suspeitas. Os burlões tentam fazer as suas mensagens parecer oficiais e familiares, para que confie nelas. Pense duas vezes quando receber uma mensagem suspeita e evite partilhar informações pessoais por mensagem ou e-mail. Elas incluem o seu endereço de casa, informações bancárias, palavras-passe, etc. Não clique em ligações nem transfira um ficheiro se não conhecer ou não confiar no remetente. Prática número dois: procure sinais de que a página Web é segura. Antes de fornecer informações de cartão de crédito, inserir uma palavra-passe ou fornecer outras informações pessoais, verifique se se encontra num site seguro e fidedigno. A maioria dos sites seguros têm o prefixo HTTPS no início do URL, na barra de endereços do browser. Além disso, certifique-se de que está na página Web certa. Os burlões tentam muitas vezes conduzi-lo a páginas Web que parecem ser oficiais, usando nomes de empresas com erros ortográficos para o enganar. www.microsoft.net não é o mesmo que o site oficial da Microsoft, em <www.microsoft.com>. Verifique sempre o URL para se certificar de que está na página Web certa. Prática número três: mantenha o seu browser e o sistema operativo atualizados. Pode ativar as atualizações automáticas para garantir que as versões mais recentes do software são instaladas automaticamente no seu computador. Manter o software do dispositivo atualizado significa que receberá as mais recentes atualizações de segurança, que ajudam a proteger o seu computador. Prática número quatro: instalar software anti-malware verificado nos seus dispositivos. Trata-se de um software especial, projetado para proteger o seu computador contra os hackers e software nocivo. Não seja o próximo peixe a ser apanhado no anzol. Ao utilizar a Internet, lembre-se de pensar antes de clicar, transferir ou partilhar, para se proteger de esquemas de phishing online.

## Comunicar com segurança online

2 minutos

### Comunicar com segurança online

A internet permite-nos comunicar com outras pessoas de novas formas. No entanto, nem sempre é seguro comunicar com outras pessoas online. Nem sempre se sabe com certeza com quem se fala quando se está na internet, por isso temos de ter cuidado para nos mantermos seguros.

**Veja o seguinte vídeo para aprender a comunicar com segurança online.**

### Vídeo: Comunicar com segurança online

Utilizando a Internet podemos comunicar de novas formas com outras pessoas em todo o mundo. Isso apresenta muitos benefícios, mas também alguns perigos. Há predadores online que usam a Internet diariamente. Com frequência estes predadores fingem ser quem não são. Assim, pode ser difícil saber com quem está a falar online. Eis três dicas para se proteger contra predadores ao comunicar online. Dica número um: utilize o seu instinto. Se alguém o faz sentir-se nervoso ou desconfortável, pare de comunicar com essa pessoa e informe de imediato alguém em quem confie. A maioria dos Websites e sites de redes sociais possuem ferramentas para reportar atividades suspeitas. Dica número dois: limite o que partilha. Com frequência os predadores online tentam fazer com que partilhe as suas informações pessoais através de e-mails e mensagens. Evite partilhar informações pessoais com estranhos online. Dica número três: mantenha a distância. Pense duas vezes antes de conhecer pessoalmente alguém com quem só falou online. Os predadores online usam com frequência as redes sociais para fingir ser outra pessoa, criando perfis falsos usando fotografias de outras pessoas. Mesmo que alguém pareça amigável, pode ser difícil saber com certeza com quem está a falar online. Informe sempre os seus pais ou alguém em quem confie se um estranho online pedir para o conhecer pessoalmente, de modo a evitar situações perigosas. Muitos predadores online usam táticas inteligentes para o atrair para situações perigosas, mas pode ser mais inteligente que eles. Lembre-se destes riscos e dicas para se manter em segurança ao falar com alguém online.

## Criar senhas fortes

2 minutos

### Criar senhas fortes

Uma grande parte de se manter seguro e manter a sua informação privada on-line é proteger as suas informações, as suas contas e o seu computador usando senhas fortes.

**Veja o vídeo seguinte para aprender a criar senhas fortes e eficazes que possam proteger as suas informações.**

### Vídeo: Criar senhas fortes

As palavras-passe protegem as suas contas e informações pessoais de outras pessoas. Uma palavra-passe é tão importante como a fechadura de uma porta. Deve possuir uma fechadura forte, difícil de forçar e que impeça a entrada de pessoas perigosas. Também não quer que ninguém encontre as chaves da sua fechadura. Uma palavra-passe segura é como uma fechadura segura para a sua conta: quer que seja difícil para os outros adivinharem, mas também quer que seja segura e mantê-la protegida para que os outros não a possam encontrar. Siga estas dicas para criar palavras-passe seguras e para as manter protegidas. Dica número um: use uma combinação de letras, números e símbolos na sua palavra-passe. Usar uma combinação de letras maiúsculas e minúsculas e carateres e acrescentar números permite melhorar a segurança da sua palavra-passe. Dica número dois: evite usar palavras comuns na sua palavra-passe. Isso inclui palavras e expressões comuns, como palavra-passe ou website, e palavras-chave pessoais, como o seu aniversário, nome ou cidade natal. Os hackers podem adivinhar estas expressões na sua palavra-passe. Uma combinação exclusiva de carateres e números permite criar uma palavra-passe mais segura. Dica número três: use palavras-passe diferentes para as diversas contas. Se alguém adivinhar a sua palavra-passe do e-mail, a sua segurança e privacidade poderão ficar comprometidas se utilizar a mesma palavra-passe para a sua conta bancária. Em vez disso, use palavras-passe diferentes para cada uma das suas contas online. Dica número quatro: a sua palavra-passe é exclusivamente sua. Se a partilhar com outras pessoas, ainda que familiares e amigos, é mais provável que outra pessoa a utilize ou não a mantenha segura. Guarde as suas palavras-passe para si. Ao iniciar sessão nas contas, certifique-se de que as encerra quando terminar e não guarde as informações de início de sessão em computadores públicos. Além disso, evite fazer negócios pessoais em computadores ou redes públicos: isso facilita o acesso dos hackers às suas informações. Recorde que usar palavras-passe seguras e mantê-las protegidas é importante para a sua segurança e privacidade online. Tenha presentes estas dicas ao criar uma nova palavra-passe.

## Descreva as melhores práticas para partilhar informações online

2 minutos

### Seja inteligente quando partilhar

Quando estamos online, muitas vezes podemos fazer muitas coisas que ameaçam a nossa segurança sem pensar muito nisso. É importante pensar duas vezes sobre o que partilha online e manter a sua segurança em mente.

**Veja o seguinte vídeo para saber mais sobre os riscos de partilha excessiva online.**

### Vídeo: Oversharing online

A Internet e a Web permitem-nos ficar ligados aos familiares e amigos em todo o mundo. Podemos usar as redes sociais e outras plataformas para ver o que está a acontecer nas vidas dos nossos amigos, partilhar notícias pessoais e mantermo-nos em contacto com os outros, mas partilhar coisas online nem sempre é seguro. Considere este cenário: Harold compra um carro novo e quer que os amigos o vejam. Para isso, publica uma fotografia nas redes sociais. Isto pode parecer inofensivo, mas a imagem inclui muitas informações pessoais sobre Harold. Todos podem ver a sua matrícula, que tipo de carro ele conduz e onde vive, tudo numa fotografia. Pode ser inofensivo para os amigos verem, mas poderá ser perigoso se a pessoa errada encontrar estas informações e quiser usá-las de forma prejudicial. É importante pensar na segurança e privacidade ao partilhar coisas online. Ao configurar perfis em sites de redes sociais, consulte as definições de privacidade da sua conta. Se a sua conta for pública, qualquer pessoa poderá ver as suas informações e o que partilha. Em vez disso, use definições privadas para as contas, de modo a que apenas os seus contactos pessoais possam ver o que partilha. Também deverá ser seletivo ao aceitar convites para se ligar a alguém através das redes sociais. A maioria das plataformas de redes sociais tem uma forma de aceitar e recusar pedidos, permitir amigos ou seguidores no site. Quando aceita alguém, a pessoa tem acesso direto ao seu perfil e às coisas que partilha. Lembre-se disso quando receber um pedido e certifique-se de que só interage com pessoas que conhece e em quem confia. Mesmo controlando quem tem acesso aos seus perfis e contas, não consegue controlar o que as outras pessoas fazem com as suas informações. Após partilhar algo online não se pode removê-lo. Nunca partilhe algo online que não queira que estranhos e o público em geral vejam. Lembre-se sempre de pensar antes de partilhar. Pense sempre na sua segurança e faça escolhas inteligentes ao partilhar algo online.

### Experimente por si mesmo.

O que aprendeu com este vídeo? Escreva 1-3 coisas que terá em mente quando partilhar informações pessoais online.

## Descreva a importância de gerir a sua pegada digital

3 minutos

### A sua pegada digital

Há muito que podemos fazer online, desde navegar na web, partilhar atualizações nas redes sociais, fazer compras online. Deve ter em mente que tudo o que faz online faz parte da sua história online ou da sua **pegada digital.**.

Deve pensar na sua pegada digital quando partilha informações ou faz coisas online porque as coisas que acontecem online são difíceis de apagar.

**Veja o seguinte vídeo para saber mais sobre a sua pegada digital e como geri-la.**

### Vídeo: Gerencie a sua pegada digital

Se utiliza a Internet, deverá estar ciente da sua pegada digital. Assim como as pegadas físicas que mostram que alguém andou num caminho de terra batida, a sua pegada digital conta uma história de toda a sua atividade online. Todas as suas publicações nas redes sociais, todos os Websites que visita e todas as informações que partilha online contribuem para a sua pegada digital. Quando publica algo online, não é possível eliminá-lo. Assim, a sua pegada digital pode durar para sempre. Isso poderá ser uma coisa boa, se a sua pegada digital incluir coisas que lhe deem uma reputação online positiva. Isso poderá ajudá-lo a construir a sua marca pessoal. O seu histórico online também pode ajudar as aplicações que utiliza a saberem mais sobre si. Elas podem usar estas informações para o servir melhor, ajustando-se às coisas de que gosta e aos seus hábitos diários. Mas também podem usar estas informações de forma errada, partilhando-as com outros. Tenha presentes as seguintes dicas ao estar online, de modo a gerir a sua pegada digital. Dica número um: saiba o que a sua pegada diz sobre si. As outras pessoas usam a sua pegada digital para fazer juízos sobre si online. Pode incluir empregadores, quando se candidata a um emprego, ou recrutadores quando se candidata a programas académicos. É importante saber o que a sua pegada digital diz sobre si e como as suas informações estão a ser usadas. Para ver qual é a sua marca pessoal online, pode procurar por si mesmo. Pesquise o seu nome no motor de busca Bing e veja que resultados são apresentados. Se esses resultados não mostrarem o que pretende, pense no que partilha online e em que informações permite que as outras pessoas vejam. Dica número dois: faça a gestão das suas definições de privacidade. Pode modificar as definições de privacidade da maioria dos sites de redes sociais e aplicações online que utiliza. Isso pode ajudá-lo a controlar quem vê o que partilha e que informações são apresentadas quando alguém procura por si online. Dica número três: faça a gestão dos seus cookies. Os cookies são informações transmitidas ao seu browser quando navega na Web. Os cookies ajudam as aplicações a rastrear informações de que precisam quando as utiliza. Isso pode ajudar a aplicação a funcionar melhor para si. Mas esses dados também contribuem para a sua pegada digital. Pode utilizar as definições do seu browser para limitar ou bloquear a utilização de cookies em determinados Websites. Dica número quatro: pense antes de partilhar. Quando partilha algo online, não é possível eliminá-lo. Certifique-se de que concorda que algo integre a sua pegada digital pública antes de o partilhar. A sua pegada digital pode durar para sempre. Tenha estas dicas presentes para garantir que está satisfeito com a sua pegada digital e com a forma como é usada.

Verificação de conhecimentos

3 minutos

1. Qual dos seguintes componentes deve procurar no URL de uma página web, para se certificar de que está num site seguro?

* http
* seguro
* **https - Correto! "https" significa que a página web está segura.**
* ssh

1. Qual destas senhas é a mais forte?

* **John@453- Correto! Esta palavra-passe contém maiúsculas, minúsculas, caráter especial e números.**
* john500
* JoHn300
* 125893

1. A sua pegada digital é:

* O tamanho da informação nas suas contas online.
* O número de pessoas a quem estás ligado online.
* **Um registo de tudo o que fazes e dizes online. Correto! A sua pegada digital facilita o rastreio das suas ações online.**
* O seu nome de utilizador online.
* r usando senhas fortes.

## Resumo

1 minuto

Parabéns!

Completou o módulo de segurança e privacidade online e agora pode responder as seguintes perguntas por si mesmo:

1. Quais são alguns perigos de usar a internet e a web?
2. Quais são alguns sinais de riscos de segurança e fraudes online?
3. Que medidas pode tomar para se manter seguro durante a utilização da internet?
4. Como pode gerir a sua pegada digital?

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

# Civismo online

9 minutos ! 5 unidades

Neste módulo, você vai aprender mais sobre direitos e boas práticas para usar a informação on-line. Também aprenderá sobre ciberbullying.

Introdução

1 minuto

Podemos usar a internet para aceder a muita informação e comunicar com os outros, mas temos de nos certificar de que nos comportamos como cidadãos digitais responsáveis.

Nesta lição, aprenderá a usar responsavelmente a internet e a web.

**No final desta lição, poderás:**

1. Descreva os direitos que as pessoas têm à informação e conteúdo partilhado na web.
2. Descreva as melhores práticas para a utilização de informações encontradas na web.
3. Descreva as implicações de tratar mal os outros na web.
4. **proteger a sua informação.**

## Descreva as melhores práticas para usar informações encontradas na web

2 minutos

### Use a informação de forma responsável

Embora o acesso à informação seja fácil no mundo digital, existem algumas regras a ter em mente quando se quer usar a informação que encontra online.

**Veja o seguinte vídeo para saber algumas das diretrizes para usar informações que encontre online.**

### Vídeo: Use a informação de forma responsável

A Internet oferece-nos informação e possibilidades ilimitadas. Podemos encontrar tudo, desde vídeos engraçados até às nossas músicas favoritas ou informações sobre como resolver um problema dos trabalhos de casa, mas devemos ser responsáveis relativamente às informações que encontramos online. Considere este cenário. Harold quer escrever um livro de receitas e vendê-lo online. Como não é bom a tirar fotografias, procura imagens online. Transfere imagens de diversos alimentos e inclui-as no seu livro. Isto pode parecer correto, pois é fácil de fazer, mas esta não é uma forma justa nem responsável de usar informações encontradas online. Quando alguém coloca o seu trabalho original online, incluindo as suas palavras, imagens, vídeos, música e muito mais, torna-se proprietário desses conteúdos. Como proprietário tem determinados direitos, geralmente considerados direitos de autor, para decidir como esses conteúdos podem ser usados. Usar as palavras ou o trabalho de outra pessoa como se fossem seus é considerado plágio. Isso não é justo para o autor original e pode trazer-lhe problemas a si. Se quiser usar os conteúdos de outra pessoa no seu trabalho, certifique-se de que o refere, dando-lhe crédito pelo seu trabalho. Ao usar o trabalho de alguém num produto que esteja a vender, deverá obter primeiro a permissão do autor. Também poderá ter de pagar por uma licença para usar o trabalho de alguém. Por vezes os autores de conteúdos disponibilizam o seu trabalho de forma gratuita. Pode usar motores de pesquisa como o Bing para procurar imagens, conteúdos multimédia e outros tipos de conteúdos que estejam disponíveis para outros utilizarem. Ao usar a Internet e procurar informações online, certifique-se de que as utiliza de forma justa e responsável.

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

3 minutos

### Ciberbullying

A internet permite-nos conectar-nos com outros online de todo o mundo. Infelizmente, as pessoas nem sempre se tratam bem online.

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

**Veja o seguinte vídeo para aprender dicas para prevenir o ciberbullying e ser um cidadão digital.**

### Vídeo: Trate os outros respeitosamente online

A Internet e as plataformas das redes sociais ligam-nos aos nossos familiares, amigos e colegas de formas inovadoras. Por vezes as pessoas tiram partido destas plataformas, usando-as para disseminar mensagens negativas sobre os outros.

O cyberbullying, ou bullying que ocorre na Internet, pode ser tão mau como o bullying em pessoa. As pessoas podem usar a Internet para enviar mensagens negativas a alguém, espalhar rumores falsos ou partilhar informações privadas de alguém sem a sua permissão. Quando alguém sofre cyberbullying, os seus sentimentos podem ser feridos e a sua reputação pode ser prejudicada. Nem sempre é possível evitar o ciberbullying, mas pode desempenhar um papel em tornar a Internet um local mais amigável e mais seguro para todos.

Eis algumas orientações que poderá seguir para promover o civismo digital online:

* Viva de acordo com a Regra de Ouro. Trate os outros como gostaria de ser tratado, seja presencialmente, seja online.
* Evite enviar mensagens negativas e participar em comportamentos que possam magoar outras pessoas.
* Respeite as diferenças. Somos todos diferentes em muitos aspetos. Ao interagir com pessoas online, respeite as suas diferenças de opinião, experiência e cultura. Mesmo que não concorde com algo que outra pessoa partilhe online, deverá continuar a tratá-la com respeito, tornando a Internet num espaço de comunicação amigável.
* Faça uma pausa antes de responder. Antes de partilhar algo online, para sempre para pensar nas consequências. A sua mensagem magoará alguém? Prejudicará a sua reputação ou a segurança ou reputação de outros?
* Pense duas vezes antes de partilhar algo online. Defenda-se a si próprio e aos outros. Se se sentir inseguro online, deverá sentir-se à vontade para se retirar de uma situação e para a denunciar a alguém em quem confie.
* Se testemunhar atividades cruéis ou perigosas online, ofereça apoio aos envolvidos e reporte o incidente a alguém em quem confie. Todos podemos desempenhar um papel em tornar a Internet num lugar seguro e amigável para todos.
* Faça a sua parte e seja um cidadão digital responsável online.

## Verificação de conhecimentos

2 minutos

1. Qual destas ações não está a violar direitos de autor?

* Usando as imagens de alguém num livro que publica sem a sua permissão.
* **Citando um parágrafo do livro de alguém e referindo-se a eles - Correto! Observa os direitos de autor quando cita o proprietário.**
* Vender o vídeo de alguém com o seunome.
* Vender o livro de alguém semlicença.

1. O cyberbullying pode ocorrer:

* Só nas plataformas das redes sociais.
* Só através de e-mails.
* Só na SMS.
* **Nas plataformas de redes sociais e SMS, e através de e-mails. Correto! O cyberbullying pode ocorrer em qualquer tipo de comunicação online.**

## Resumo

1 minuto

Parabéns!

Completou o módulo de civismo Online e agora pode responder as seguintes perguntas por si mesmo:

1. O que deve fazer quando pretende usar informações que encontra online?
2. O que se pode fazer para prevenir ou acabar com o ciberbullying?

# Imprima o seu certificado

2 minutos ! 2 unidades

Tem de completar todos os módulos deste curso para receber o seu certificado.

## Receber crédito

1 minuto

### Completo

Parabéns por concluir Participar de forma segura e responsável online. Selecione **Receber crédito** para completar o curso e receber o seu certificado.

### Crédito recebido

Parabéns por concluir Participar de forma segura e responsável online..

Na caixa abaixo, escreva o seu nome como gostaria que aparecesse no seu certificado e selecione **o certificado 'Ver'.**.