Alfabetização Digital

Transcrição

Participar com segurança e responsabilidade on-line

Neste caminho de aprendizado, você conhecerá os riscos de segurança que pode enfrentar ao usar a Internet. Você aprenderá 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.

Este arquivo traz a transcrição do áudio de todos os vídeos que fazem parte deste curso para que você possa, sempre que precisar, acessar um conteúdo específico e rever os conceitos apresentados.

*Você pode usar o **Sumário,** clicando no número da página, para acessar diretamente o Módulo e o tema que procura.*

Bons estudos!

Sumário

Módulo 1 – Segurança e privacidade on-line

Proteja-se do phishing

Vídeo: Proteja-se do phishing

A Internet nos traz muitas possibilidades. Podemos conversar com outras pessoas, fazer compras on-line e fazer negócios pessoais em um só lugar. Mas essas interações on-line nem sempre são seguras. Vamos falar sobre um golpe on-line popular do qual você precisa estar ciente.

Uma maneira comum de pegar um peixe é colocar a comida no anzol para que o peixe queira comê-la. Depois de morderem a comida, eles serão fisgados. Os golpes de phishing na Internet funcionam da mesma maneira. Pessoas que querem roubar suas informações são como pescadores. Eles enviam um e-mail ou mensagem instantânea por meio de um site de mídia social ou um jogo on-line. Frequentemente, fingem ser alguém que não são e pedem informações privadas ou dizem para você clicar em um hiperlink para que você possa concluir uma tarefa importante. Se você fornecer as informações ou clicar no hiperlink, você será fisgado. Mas não se preocupe. Essas quatro práticas podem ajudar a protegê-lo contra golpes de phishing.

Prática número um: tenha cuidado com mensagens suspeitas. Os golpistas tentam fazer com que suas mensagens pareçam oficiais e familiares, para que você confie neles. Pense duas vezes ao receber uma mensagem suspeita e evite compartilhar informações pessoais por mensagem ou e-mail. Isso inclui seu endereço residencial, informações bancárias, senhas e muito mais. Não clique em um link ou 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 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 endereço do navegador. Além disso, verifique se você está na página Web correta. Os golpistas costumam tentar levá-lo a páginas da web que parecem ser oficiais e usam nomes de empresas incorretos para enganá-lo. www.microsoft.net não é o mesmo que o site oficial da Microsoft em www.microsoft.com.

Sempre verifique a URL para certificar-se de que você está na página correta.

Prática número três: mantenha seu navegador da web e sistema operacional atualizados. Você pode ativar as atualizações automáticas para garantir que as versões de software mais recentes sejam instaladas automaticamente no computador. Manter o software do seu dispositivo atualizado significa que você receberá as atualizações de segurança mais recentes que ajudam a proteger o seu computador.

Prática número quatro: instale um software antivírus em seus dispositivos. Este é um software especial projetado para proteger seu computador de softwares prejudiciais e hackers. Não seja o próximo peixe a ser fisgado. Ao usar a Internet, lembre-se de pensar antes de clicar, fazer download ou compartilhar para se proteger contra golpes de phishing on-line.

Comunique-se com segurança on-line

Vídeo: Comunique-se 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 existem alguns perigos. Existem predadores on-line que usam a Internet todos os dias. Esses predadores muitas vezes fingem ser pessoas que não são. Portanto, pode ser difícil saber com quem você está falando on-line. Aqui estão três dicas que você pode usar para se manter protegido de predadores on-line ao se comunicar on-line.

Dica número um: use seus instintos. Se alguém deixar você nervoso ou desconfortável, pare de se comunicar com essa pessoa e diga a alguém em quem você confia imediatamente. A maioria dos sites e redes de mídia social têm ferramentas que você pode usar para relatar atividades suspeitas.

Dica número dois: limite o que você compartilha. Predadores on-line frequentemente tentam fazer com que você compartilhe suas informações pessoais por meio de e-mails e mensagens. Evite compartilhar informações pessoais com um estranho on-line.

Dica número três: mantenha distância. Pense duas vezes antes de conhecer pessoalmente alguém com quem você só conversou on-line. Predadores on-line costumam usar a mídia social para fingir ser outra pessoa, criando perfis falsos usando fotos de outras pessoas. Mesmo que alguém pareça amigável, pode ser difícil saber com certeza com quem você está falando on-line. Sempre diga a seus pais ou alguém de sua confiança quando um estranho on-line pedir para conhecê-lo pessoalmente, para que você não acabe em uma situação perigosa. Muitos predadores on-line usam táticas inteligentes para atraí-lo para situações perigosas, mas você pode ser mais esperto.

Lembre-se desses riscos e dicas para ficar seguro ao falar com as pessoas on-line.

Criar senhas fortes

Vídeo: Criar senhas fortes

As senhas ajudam a proteger suas informações pessoais e contas de outras pessoas. Uma senha é tão importante quanto a fechadura de uma porta. Você quer uma fechadura forte que seja difícil de quebrar e evitar que pessoas perigosas entrem. Você também não quer que ninguém encontre as chaves da sua fechadura. Uma senha forte é como um cadeado forte para sua conta, você quer que seja difícil para outras pessoas adivinhá-la, você também quer que ela esteja segura e protegida para que outros não possam encontrá-la. Siga estas 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 ainda, adicionar números pode melhorar a força de sua senha.

Dica número dois: evite usar palavras comuns em sua senha. Isso inclui palavras e frases comuns como "senha" ou "site da Web", bem como palavras-chave pessoais como seu aniversário, seu nome ou sua cidade natal. Os hackers podem adivinhar facilmente essas frases em sua senha. Uma combinação única de caracteres e números cria uma senha mais forte.

Dica número três: use senhas diferentes para contas diferentes. Se alguém adivinhar sua senha de e-mail, sua segurança e privacidade podem estar em perigo se você usar a mesma senha para sua conta bancária. Em vez disso, use senhas diferentes para cada conta on-line que você possui.

Dica número quatro: sua senha é apenas sua. Quando você compartilha sua senha com outras pessoas, mesmo com amigos e familiares, é mais provável que outra pessoa a use ou não a mantenha segura. Guarde suas senhas para você. Ao fazer login em contas, certifique-se de sair quando terminar e não salve suas informações de login em um computador público.

Além disso, evite fazer negócios pessoais em computadores e redes públicas, pois isso torna mais fácil para os hackers acessarem suas informações. Lembre-se de que usar senhas fortes e mantê-las protegidas é importante para sua segurança e privacidade on-line. Lembre-se dessas dicas ao criar uma nova senha.

Conhecer as melhores práticas para compartilhar informações on-line

Vídeo: Compartilhar on-line

A Internet e a web permitem que permaneçamos conectados com amigos e familiares em todo o mundo. Podemos usar a mídia social e outras plataformas para ver o que está

acontecendo na vida de nossos amigos, compartilhar notícias pessoais e manter contato com outras pessoas, mas compartilhar coisas on-line nem sempre é seguro.

Considere este cenário, Harold compra um carro novo e quer que seus amigos o vejam. Então, ele posta uma foto dele nas redes sociais. Isso pode parecer bom, mas a imagem inclui muitas informações pessoais sobre Harold. Qualquer pessoa pode ver o número da placa de seu carro, que tipo de carro ele dirige e onde mora a partir de uma foto.

Pode ser que seus amigos vejam isso, mas pode ser perigoso se a pessoa errada encontrar essa informação e quiser usá-la de maneira inadequada. É importante manter a segurança e a privacidade em mente ao compartilhar coisas on-line.

Ao configurar perfis em sites de mídia social, certifique-se de revisar as configurações de privacidade de sua conta. Se sua conta for definida como pública, qualquer pessoa poderá ver suas informações e o que você compartilha. Em vez disso, use a configuração privada nas contas, para que apenas as suas conexões pessoais vejam o que você compartilha.

Você também deve ser seletivo ao aceitar convites para se conectar com alguém através da mídia social. A maioria das plataformas de mídia social tem uma maneira para você aceitar e negar solicitações, para ter alguém como seu amigo ou seguidor no site. Depois de aceitar alguém, essa pessoa tem acesso direto ao seu perfil e às coisas que você compartilha. Lembre-se disso ao receber uma solicitação e certifique-se de interagir apenas com pessoas que conhece e em quem confia.

Mesmo quando você controla quem tem acesso aos seus perfis e contas, não pode controlar o que outras pessoas fazem com suas informações. Quando você compartilha algo on-line, você não pode apagá-lo. Nunca compartilhe algo on-line que você não gostaria que estranhos e o público vissem. Lembre-se sempre de pensar antes de compartilhar. Mantenha sua segurança em mente e faça escolhas inteligentes ao compartilhar coisas on-line.

Conhecer a importância de gerenciar sua pegada digital

Vídeo: Gerenciar sua pegada digital

Se você usa a Internet, deve estar ciente de sua pegada digital. Assim como pegadas físicas que mostram alguém pisando em um caminho de terra, sua pegada digital é um histórico de todas as atividades que você realiza on-line. Quaisquer postagens de mídia social que você faça, qualquer site que visite e qualquer informação que você compartilhe on-line contribui para sua pegada digital.

Depois de postar algo on-line, ele não pode ser apagado. Portanto, sua pegada digital pode durar para sempre. Isso pode ser bom se sua pegada digital incluir coisas que dão a você uma reputação positiva on-line. Isso pode ajudá-lo a construir sua marca pessoal.

Seu histórico on-line também pode ajudar os aplicativos que você usa a saber mais sobre você. Eles podem usar essas informações para atendê-lo melhor, ajustando-se às coisas de que você gosta e aos seus hábitos diários. Mas eles também podem usar essas informações de maneira errada e compartilhá-las com outras pessoas. Lembre-se das dicas a seguir quando estiver on-line 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 on-line. Isso pode incluir empregadores quando você se candidatar a um emprego ou recrutadores quando se candidatar a programas acadêmicos. É importante saber o que sua pegada digital diz sobre você e como suas informações estão sendo usadas. Para ver o que sua marca pessoal é on-line, você pode pesquisar por si mesmo. Pesquise seu nome no mecanismo de pesquisa Bing e veja quais resultados são exibidos. Se esses resultados não mostrarem o que você deseja, pense no que você compartilha on-line e quais informações 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 on-line que você usa. Isso pode ajudá-lo a controlar quem vê o que você compartilha e quais informações são exibidas quando alguém procura por você on-line.

Dica número três: gerencie seus cookies. Cookies são notas fornecidas ao seu navegador enquanto você navega na web. Esses cookies ajudam os aplicativos a rastrear as informações de que precisam enquanto você está usando o aplicativo. 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 seu navegador para limitar ou bloquear o uso de cookies em determinados sites.

Dica número quatro: pense antes de compartilhar. Depois de compartilhar algo on-line, você não pode retirá-lo. Certifique-se de que você concorda com algo que faz parte de sua pegada digital pública antes de compartilhá-lo. Sua pegada digital pode durar para sempre. Lembre-se dessas dicas para ter certeza de que está satisfeito com sua pegada digital e como ela é usada.

Módulo 2 – Cidadania Digital

Conhecer as melhores práticas para usar informações encontradas na web

Vídeo: Usar as informações de forma responsável

A Internet nos dá informações e possibilidades ilimitadas. Podemos encontrar de tudo, desde vídeos engraçados até nossas músicas favoritas ou informações sobre como resolver um problema de lição de casa, mas devemos ser responsáveis com as informações que encontramos on-line.

Considere este cenário. Harold quer escrever um livro de receitas e vendê-lo on-line. Ele não é bom em tirar fotos, então ele pesquisa imagens on-line. Ele baixa imagens de diferentes alimentos e as inclui em seu livro. Isso pode parecer normal porque é fácil de fazer, mas não é uma forma justa ou responsável de usar as informações encontradas on-line.

Quando alguém coloca seu trabalho original on-line, incluindo palavras, imagens, vídeos, música e outros, ele se torna o proprietário do conteúdo. Como proprietário, ele tem certos direitos, geralmente considerados direitos autorais, para decidir como o conteúdo pode ser usado. Se você usar as palavras de outra pessoa ou usá-las como se fossem suas próprias palavras, isso é considerado plágio. Isso não é justo para o autor original e pode causar problemas. Se você quiser usar o conteúdo de outra pessoa em seu trabalho, certifique-se de referenciá-la e dar-lhe crédito por seu trabalho.

Ao usar o trabalho de alguém em um produto que está vendendo, primeiro você deve obter permissão do autor. Você também pode ter que pagar uma licença para usar o trabalho de alguém. Às vezes, os autores do conteúdo disponibilizam seu trabalho para uso gratuito.

Você pode usar mecanismos de pesquisa como o Bing para localizar imagens, mídia e outros tipos de conteúdo que estão disponíveis para uso de terceiros. Ao usar a Internet e encontrar informações on-line, certifique-se de usá-la de forma justa e responsável.

Conhecer as implicações de tratar mal os outros na web

Vídeo: Trate os outros com respeito on-line

A Internet e as plataformas de mídia social nos conectam com nossos amigos, familiares e colegas de novas maneiras. Às vezes, as pessoas aproveitam essas plataformas e as usam para espalhar mensagens negativas sobre os outros.

O cyberbullying, ou bullying que ocorre na Internet, pode ser tão ruim quanto o bullying em pessoa. As pessoas podem usar a Internet para enviar mensagens maldosas a alguém,

espalhar boatos falsos ou compartilhar informações privadas de alguém sem permissão. Quando alguém é vítima de cyberbullying, seus sentimentos podem ser feridos e sua reputação pode ser prejudicada. Nem sempre é possível prevenir o cyberbullying, mas você pode contribuir para tornar a Internet um lugar mais amigável e seguro para todos.

Aqui estão algumas diretrizes que você pode seguir para promover a cidadania digital on-line:

- Viva pela Regra de Ouro. Trate os outros da maneira como você deseja ser tratado, seja pessoalmente ou on-line.
- Evite enviar mensagens negativas e participar de comportamentos que possam magoar outra pessoa.
- Respeite as diferenças. Somos todos diferentes de muitas maneiras. Ao interagir com pessoas on-line, respeite suas diferenças de opinião, experiência e cultura. Mesmo se você não concordar com algo que outra pessoa compartilha on-line, você ainda deve tratá-la com respeito e fazer da Internet um espaço amigável de comunicação.
- Faça uma pausa antes de responder. Antes de compartilhar qualquer coisa on-line, sempre pare e pense nas consequências. A sua mensagem magoará outra pessoa? Isso prejudicará sua reputação ou a segurança ou reputação de outras pessoas?
- Pense duas vezes antes de compartilhar on-line. Defenda você mesmo e os outros. Se não se sentir seguro on-line, você deve se sentir confortável para sair de uma situação e relatá-la a alguém de sua confiança.
- Quando você vir atividades cruéis ou perigosas on-line, ofereça suporte aos envolvidos e relate o incidente a alguém de sua confiança. Todos nós podemos contribuir para tornar a Internet um lugar seguro e amigável para todos.
- Faça a sua parte e seja um cidadão digital responsável.