Wi-Fi público

Os participantes aprenderão sobre redes Wi-Fi públicas e suas vantagens e desvantagens. Mais especificamente, eles aprenderão a reconhecer Wi-Fi disponíveis que não estão protegidos, a entender as diferenças que existem no uso de Wi-Fi não protegido e a tomar decisões fundamentadas em relação à conexão e ao uso de Wi-Fi não protegido.

Recursos

Imagem de modem sem fio
Segurança da conexão

O que é Wi-Fi?

Parte 1

Pergunte aos seus alunos

Quais dispositivos você usa para acessar a internet?

Como esses dispositivos se conectam à internet?

Interação de classe de imagem

Wi-Fi é uma maneira comum de conectar os dispositivos à internet. O Wi-Fi usa sinais de rádio para conectar dispositivos sem uma conexão física ou com fio.

Imagine que você tem três laptops em casa que gostaria de conectar à internet. Para isso, você precisará do seguinte:

1. Um ponto de acesso: ponto de acesso é qualquer coisa que transmita um sinal Wi-Fi e ofereça acesso à internet. Seus dispositivos precisam captar esses sinais para fazer a conexão com a internet. Às vezes você precisa de permissão especial (por exemplo, um nome de usuário e uma senha) para fazer a conexão e usar o sinal sem fio transmitido pelo ponto de acesso.

2. Um roteador: roteador é um dispositivo que cria uma rede entre todos os dispositivos (por exemplo, computadores, tablets, celulares) em um local (como uma escola, biblioteca ou em sua casa). Normalmente, os roteadores têm um ponto de acesso interno (confira o diagrama acima).

> Eles têm um alcance limitado (normalmente curto). É por isso que você recebe um sinal fraco de Wi-Fi, ou até nenhum, quando está muito longe do roteador. Além disso, se houver algo entre você e o roteador (como um prédio ou uma parede de tijolos), isso reduzirá seu sinal.
>
> Embora a conexão com um roteador ofereça acesso a uma rede, isso não significa necessariamente acesso à internet. Para que vários dispositivos em uma rede tenham acesso à internet, o roteador precisa estar conectado a um modem.

3. Um modem: modem é um dispositivo que cria e mantém uma conexão com sua operadora de internet (ISP) para oferecer acesso à internet. Ele converte sinais externos em sinais que podem ser lidos por seu computador e por outros dispositivos digitais.

> Em uma configuração padrão, o ponto de acesso e o roteador são um mesmo

dispositivo que está fisicamente acoplado ao modem com um cabo especial chamado Ethernet. É disso que as pessoas estão falando quando falam sobre conexões de internet “com fio”.

Os dispositivos móveis também podem usar uma conexão celular para conexão à Internet, especialmente se não estiverem na rede do colégio, da biblioteca ou de casa. As conexões celulares são um tipo de sinal de rádio sem fio com área de cobertura muito mais ampla que a de um roteador. As conexões celulares usam transmissores-receptores, chamados torres de celular, para conectar seu dispositivo móvel à internet.

Parte 2

Pergunte aos seus alunos

Quais são as vantagens do Wi-Fi?

Quais são as desvantagens do Wi-Fi?

Quais são as questões de segurança envolvidas no uso do Wi-Fi se comparado com uma conexão de Internet com fio?

Por que você perde acesso ao Wi-Fi em seu telefone ao sair do prédio?

Como escolher uma rede Wi-Fi

Parte 1

Pergunte aos seus alunos

Todas as redes Wi-Fi são seguras? Por que sim ou por que não?

Fale para seus alunos

Às vezes, você pode escolher a rede de Wi-Fi que deseja usar. É importante saber que há riscos graves quando você se conecta a uma rede errada. Por exemplo, as redes Wi-Fi não protegidas são as que não exigem senha para acesso. Se você está em uma rede não protegida, é possível que outras pessoas na mesma rede vejam suas informações. Elas podem roubar informações enviadas pela rede ou monitorar o que você está fazendo.

Já as redes Wi-Fi protegidas e confiáveis são as que exigem senha, têm criptografia habilitada e as que você sabe que correspondem realmente ao nome da rede. Por exemplo, se você se conectar a uma rede que tem o nome da rede de seu colégio, suas informações de conta poderão ser divulgadas. Assim, as redes protegidas e confiáveis são as que oferecem maior proteção.

Pense no contexto ou na localização da rede Wi-Fi. Por exemplo, se você está no cinema e vê o nome da rede do colégio em seu telefone na hora de procurar uma conexão Wi-Fi, é bem possível que essa rede esteja tentando imitar ou "personificar" a rede do colégio para coletar senhas de alunos desatentos.

Ao configurar uma rede Wi-Fi protegida por senha, o proprietário precisa ativar o protocolo de criptografia do roteador. Dentre os protocolos de criptografia comuns estão o Wired Equivalent Privacy (WEP), o Wi-Fi Protected Access (WPA) ou o WPA2. Esses protocolos fazem com que as informações enviadas sem fio pela rede estejam criptografadas (ou "embaralhadas").

A criptografia foi criada para dificultar a visualização do que você envia pelos invasores. No entanto, todos esses protocolos (WEP, WPA e WPA2) já demonstraram que são vulneráveis a ataques. Assim, é importante usar também conexões web protegidas na hora de transmitir informações online.

HTTPS é um padrão usado por sites para criptografar dados transmitidos pela internet. A criptografia pode evitar que terceiros visualizem os dados de sua conexão. Ela oferece uma camada adicional de segurança e pode ser usada em qualquer navegador com a adição de "http://" na frete da URL utilizada (por exemplo, https://www.mysite.com). No entanto, nem todos os sites aceitam HTTPS.

1. Insira informações confidenciais (por exemplo, senhas, informações de cartão

de crédito) apenas em páginas da web com prefixo HTTPS://.

2. A maioria dos navegadores têm indicadores de segurança em formato de cadeado ao lado da barra de endereços para indicar as conexões HTTPS.

3. Infelizmente, HTTPS não garante segurança total, já que alguns sites mal-intencionados também aceitam HTTPS. O HTTPS protege a conexão, mas não é garantia de que o site seja genuíno.

Fale para seus alunos

Secure Sockets Layer (SSL)/Transport Layer Security (TLS) são os nomes das tecnologias que protegem o HTTPS. SSL/TLS usam chaves de criptografia, que funcionam de forma bem semelhante a chaves reais. Se você escrever um segredo em um pedaço de papel para seu amigo, quem encontrar o papel verá seu segredo. Mas e se você der a ele uma cópia da chave pessoalmente e enviar o segredo em caixas trancadas iguais? Se alguém interceptar a caixa, terá dificuldade em ver o segredo sem a chave. Se alguém tentar substituir a caixa por uma semelhante, você notará se a chave funciona ou não. O SSL/TLS funciona da mesma maneira, mas em um site.

Os indicadores de segurança do navegador também comunicarão as informações de certificado de Validação Estendida (EV). Os certificados EV são conferidos a sites que confirmam suas identidades junto a uma autoridade certificada. Nos navegadores, o indicador de EV às vezes tem o formato do nome do site ou da entidade de registro ao lado da barra de endereços. Se você suspeita do conteúdo de um site específico, verifique se a URL no certificado está de acordo com a URL no navegador clicando em “Visualizar certificado”. Pode ser útil demonstrar aos participantes, na tela de projeção, como encontrar a opção “Visualizar certificado”. Esses passos variam de acordo com o navegador. Por exemplo, no Chrome, em “Visualizar”, clique em “Desenvolvedor” e em “Ferramentas para desenvolvedores”. Em “Ferramentas para desenvolvedores”, clique na guia “Segurança” e em “Visualizar certificado”.

Pergunte aos seus alunos

O que você deve levar em conta na hora de se conectar a uma rede nova?

1. Algumas respostas: local (ou quem é o proprietário da rede), acesso (ou quem mais está conectado à rede) e atividade (ou o que você está fazendo na rede).

Quem é o proprietário da rede Wi-Fi em casa? No colégio? Na cafeteria?

1. Seus pais/tutores são donos da rede Wi-Fi de casa; os administradores e/ou o governo são donos da rede no colégio e o proprietário é dono da rede da

cafeteria.

Você conhece essas pessoas pessoalmente? Você confia nessas pessoas?

1. Debata com os participantes como podem ser os graus de confiança deles nessas pessoas.

Fale para seus alunos

Você deve conhecer a pessoa que oferece a rede Wi-Fi e confiar nela. Às vezes é possível determinar quem é o proprietário usando o SSID da rede.

O identificador SSID é o nome dado a uma rede Wi-Fi que pode ser visualizado na hora da conexão. O SSID costuma ser usado para indicar o proprietário da rede e outros detalhes sobre ela. Mas cuidado: quase todo mundo (que saiba fazer isso) pode criar um SSID. Por exemplo, alguém pode criar um SSID idêntico ao que você usa no colégio. Esse é um exemplo de se fazer passar por uma rede conhecida e confiável a fim de coletar nomes de usuário e senhas.

Saber quem está oferecendo a rede pode ajudá-lo a determinar se ela é protegida ou não. Se ela pertence a uma pessoa ou organização em quem você confia, será mais confortável conectar-se a essa rede. No entanto, se a rede for desconhecida, não se conecte, já que você não sabe de quem é o roteador. Como todo o tráfego da rede passa pelo roteador, o proprietário poderia estar monitorando ou gravando seu tráfego de rede.

Ao se conectar ao Wi-Fi, seu dispositivo é conectado a uma rede local de dispositivos e essa rede se conecta à internet. Como seu dispositivo está trocando informações com essa rede, é importante confiar nos outros dispositivos conectados ao seu, e isso significa todos os dispositivos na rede. É que nem o trabalho em grupo do colégio: você precisa poder confiar nas outras pessoas com quem está trabalhando!

O uso de senha na rede pode limitar o número de pessoas que se conectam a ela. Isso significa que você pode ter uma ideia melhor de quem está na rede, seja sua família, seus amigos ou outros clientes da cafeteria, do que teria se a rede fosse totalmente aberta.

Sua escolha de ingressar em uma rede suspeita ou não depende dos riscos e vantagens que você quer aceitar em termos de segurança online. Pese os prós e os contras de sua conta ser invadida comparados com a vantagem de ingressar em uma rede disponível.

Pergunte aos seus alunos

Você deveria ler notícias online/blogs usando sua rede Wi-Fi em casa? No colégio? Na cafeteria?

1. Explique que o conteúdo de uma página da web normalmente não contém informações confidenciais. Você pode fazer isso em todas as redes, provavelmente.

Você deveria enviar números de cartão de crédito usando sua rede Wi-Fi em casa? No colégio? Na cafeteria? Por quê?

1. Comece uma discussão sobre a maneira mais segura de fazer isso no Wi-Fi de casa e não no Wi-Fi da cafeteria. Fale também que, embora a rede do colégio provavelmente seja confiável, pode não valer o risco, já que esse tipo de informação é bastante confidencial.

Você deveria verificar emails usando sua rede Wi-Fi em casa? No colégio? Na cafeteria?

1. Fale sobre como isso é provavelmente mais seguro de fazer na rede de casa, dependendo do conteúdo da conta de email. Por exemplo, algumas pessoas têm várias contas de email que usam para finalidades diferentes (por exemplo, emails de marketing/promoção em uma conta, emails para amigos e familiares em outra conta).

Fale para seus alunos

É melhor enviar/visualizar informações confidenciais, inclusive senhas e informações bancárias, em uma rede privada e protegida, em sites usando SSL/TLS em vez de usar uma rede pública compartilhada. Essas informações privadas estarão em risco se você enviá-las ou acessá-las em uma rede compartilhada usada por pessoas desconhecidas ou não confiáveis.

Pode não estar claro se as informações são confidenciais ou não porque privacidade é uma escolha pessoal que você precisa fazer por conta própria. É importante considerar cada situação individualmente para determinar se você deve se conectar à rede ou não. Pergunte-se se você confia no proprietário da rede, nas outras pessoas conectadas, se a atividade online e se as informações compartilhadas são adequadas antes de decidir se conectar.

Redes protegidas e não protegidas

Parte 1

Interação da classe

Observação: parte do conteúdo dessa atividade foi abordada na “Atividade 2: Como escolher uma rede Wi-Fi” Você decide se quer rever o material ou não.

Fale para seus alunos

Como mencionado anteriormente, as redes Wi-Fi não protegidas são as que não exigem senha para acesso. O uso de redes não protegidas é um risco para os dados que você transmite e recebe pela rede.

Redes Wi-Fi protegidas são as que exigem senha e têm criptografia habilitada. Quem configurou a rede é que escolhe se a rede está criptografada ou não. A criptografia embaralha as informações enviadas e recebidas pela rede e, por isso, é muito mais difícil para um invasor na mesma rede Wi-Fi ver o que você está enviando ou recebendo.

O fato de uma rede ser protegida não significa que seus dados estão seguros. É fato que é mais seguro do que usar uma rede não protegida; no entanto, um invasor resolvido pode encontrar uma forma de acessar suas informações.

Existem três protocolos de criptografia comuns para redes Wi-Fi: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) ou WPA2. Os protocolos WEP e WPA estão desatualizados e as redes que os utilizam devem ser consideradas não protegidas. Além disso, o WPA2 também já demonstrou estar vulnerável a invasões.

Para fazer com que suas informações estejam protegidas ao máximo, verifique se os sites que você está usando são criptografados com SSL/TLS.

Pergunte aos seus alunos

Alguém consegue pensar em um exemplo de rede protegida por senha já usada?

1. Alguns exemplos são o Wi-Fi de casa, o Wi-Fi do colégio e redes Wi-Fi de alguns locais públicos, como cafeterias.

Alguém consegue dar um exemplo de rede não protegida já usada?

E exemplos de rede protegida?

Fale para seus alunos

Você pode verificar se uma rede Wi-Fi está criptografada examinando as configurações de rede ou rede sem fio em seu dispositivo.

Parte 2

Interação da classe

Antes dessa experiência de aprendizagem, faça uma pesquisa na internet para analisar como verificar os tipos de criptografia de rede Wi-Fi em sistemas operacionais diferentes. Em seguida, demonstre como descobrir o tipo de criptografia usado pela rede. Por exemplo, no MacOS, clique em Preferências do sistema -> Rede -> Selecionar Wi-Fi -> Selecione o nome da rede desejada. Na guia Wi-Fi haverá uma lista de redes conhecidas e uma coluna indicando o tipo de criptografia usado.

Fale para seus alunos

Nem todas as conexões são iguais. Quando uma rede não é protegida, todos podem se conectar a ela e não fica claro quem a controla. O ingresso em uma rede não protegida te deixa vulnerável, pois as informações enviadas e recebidas, como o tráfego da web (páginas, senhas e afins), ficam sujeitas à visualização por qualquer pessoa na rede se você não está usando uma conexão SSL/TLS.

Interação da classe

Dependendo do conhecimento técnico dos participantes, você pode debater o uso de redes privadas virtuais (VPN) como camada adicional de segurança na hora de usar Wi-Fi. Consulte os links de VPN na seção Recursos para saber mais.

Como reconhecer a segurança da conexão

Título da parte

Interação da classe

Divida os participantes em grupos de 2 a 3 pessoas. Entregue o Folheto do participante: segurança da conexão e atribua um cenário a cada um dos grupos. Dê aos participantes 5 minutos para discutirem seus cenários. Em seguida, peça aos grupos para mostrarem suas respostas. As respostas estão em verde no folheto.

Tarefa

Parte 1

Atribuição

Peça aos participantes para:

1. Desenhar um cronograma de um dia normal, marcando as redes Wi-Fi às quais eles se conectam.

2. Nas redes selecionadas demonstradas no cronograma, faça com que os participantes escolham duas e, em um breve parágrafo para cada uma, descrevam a rede: quem mais está conectada a ela? Qual é o grau de segurança?

3. Além disso, para as duas redes escolhidas, faça com que os participantes descrevam as oportunidades que a conexão com essas redes oferece e os possíveis riscos associados a isso.