Dicas de segurança para o uso de rede Wi-Fi pública

Pessoas má intencionadas podem se aproveitar de sua presença online. Leia abaixo algumas dicas a serem consideradas se você precisar utilizar a rede Wi-Fi pública.

Em resposta ao surto de Coronavírus e ao fechamento das empresas e bibliotecas, estamos passando mais tempo online. Como resultado, podemos precisar utilizar a Wi-Fi pública para se conectar à Internet. Se você precisar utilizar a Wi-Fi pública, considere as recomendações a seguir do Diretor de Privacidade estadual para ajudar a proteger seus dados:

1. Confirme a rede correta.

Você precisa se conectar à rede correta. Pessoas más intencionadas podem criar redes com aparência inofensiva se observarmos o nome delas, mas que estão de fato direcionando você a se conectar a uma estrutura de rede para observar sua navegação na Internet. Significa que se você inserir senhas ou credenciais de logon em sites da Web, o hacker poderá roubar suas informações. Para se proteger, leia o nome da rede com muito cuidado e, se possível, pergunta a um funcionário ou verifique a sinalização da empresa para ter certeza de que a rede é legítima.

Redes bem conhecidas, como redes de cafeterias famosas, são menos suspeitas devido à empresa estar operando a rede como um serviço dentro seu negócio. Redes conhecidas são geralmente mais seguras do que redes Wi-Fi gratuitas que podem ser exibidas em seu celular em locais públicos.

2. Desabilite a conexão automática.

Muitos dispositivos (smartphones, laptops e tablets) possuem configurações de conectividade automática. Esta configuração permite que os dispositivos se conectem convenientemente às redes próximas. Para redes seguras não há problemas, mas seus dispositivos também podem se conectar a redes desprotegidas. Você pode desabilitar este recurso por meio das configurações de seu dispositivo. Mantenha estas configurações desabilitadas, principalmente

quando você estiver viajando para locais desconhecidos. Como precaução adicional, você pode marcar a opção “esquecer rede” depois de utilizar uma rede Wi-Fi pública.

Você também deve monitorar seu Bluetooth quando estiver em espaços públicos.
A conectividade via Bluetooth permite que vários dispositivos se comuniquem um com o outro, e um hacker pode procurar sinais de Bluetooth abertos para obter acesso a seus dispositivos. Mantenha esta função desligada em seu celular e outros dispositivos enquanto estiver em uma área desconhecida.

3. Desabilite o compartilhamento de arquivos.

Desabilite a opção de compartilhamento de arquivos enquanto estiver conectado a uma rede Wi-Fi pública. Você pode desabilitar o compartilhamento de arquivos a partir do painel de controle ou preferências do sistema, de acordo com seu sistema operacional. AirDrop é um exemplo de recurso de compartilhamento de arquivos que você deverá desabilitar. Alguns sistemas operacionais, como o Windows/PC, desabilitarão o compartilhamento de arquivos para você ao escolher a opção “público” ao se conectar a uma nova rede pública pela primeira vez.

Etapas para desabilitar o compartilhamento de arquivos

Em um PC:

1. Acesse Central de Rede e Compartilhamento.
2. Clique em Alterar as configurações de compartilhamento avançadas.
3. Desabilite o compartilhamento de arquivo e impressora.

Para Macs:

1. Acesse Preferências do Sistema.
2. Clique em Compartilhamento.
3. Desmarque todas as opções.
4. Em seguida, no Finder, clique em AirDrop e selecione Permitir que eu seja descoberto por: Ninguém.

Para o iOS, basta encontrar o AirDrop na Central de Controle e desativá-lo.

4. Utilize uma VPN.

Considere a instalação de uma VPN (Rede Virtual Privada) em seu dispositivo. Uma VPN é a opção mais segura para a privacidade digital em uma rede Wi-Fi pública. Ela criptografa

seus dados enquanto são transmitidos de e para o seu dispositivo, e age como um “túnel” de proteção de modo que seus dados não fiquem visíveis enquanto trafegam por uma rede.

5. Alerta do FBI sobre sites da Web criptografados – HTTPS.

O FBI alertou sobre sites da Web com endereços iniciados por “https”. A presença do “https” e do ícone de cadeado pressupõem que o tráfego na Web é criptografado e que os visitantes podem compartilhar dados com segurança. No entanto, os criminosos virtuais estão se aproveitando da confiança do público e atraindo pessoas a sites maliciosos que incorporam o https e parecem seguros, quando na verdade não o são.

Recomendações do FBI:

- Não confie apenas no nome em um e-mail: questione a intenção do conteúdo do e-mail.
- Se você receber um e-mail suspeito com um link de um contato conhecido, confirme a legitimidade da mensagem telefonando ou enviando um e-mail para o contato. Não responda diretamente para um e-mail suspeito.
- Procure erros ortográficos ou domínios incorretos dentro de um link (ex.: se um endereço que deveria terminar em “.gov” está terminando em “.com”).
- Não confie em um site da Web apenas porque ele contém um ícone de cadeado ou um “https” na barra de endereços do navegador.

6. Não é recomendado acessar informações confidenciais.

Mesmo por meio de uma VPN, não é recomendado acessar contas bancárias pessoais ou dados pessoais confidenciais similares, como números de Seguridade Social, em redes públicas desprotegidas. Até mesmo redes públicas protegidas podem representar risco. Faça um julgamento criterioso caso tenha que acessar estas contas em uma rede Wi-Fi pública. Para transações financeiras, pode ser melhor utilizar a função hotspot de seu smartphone.

7. Seguras ou inseguras.

Existem basicamente dois tipos de redes Wi-Fi públicas: seguras e inseguras.

Sempre que possível, conecte-se a redes públicas seguras. É possível se conectar a uma rede insegura sem qualquer tipo de recurso de segurança, como senha ou login. Uma rede segura exige que o usuário concorde com os termos e condições, cadastre uma conta ou digite uma senha antes de se conectar.

8. Mantenha seu firewall habilitado.

Se você estiver usando um laptop, mantenha seu firewall habilitado enquanto estiver utilizando redes Wi-Fi públicas. Um firewall age como uma barreira que protege o seu dispositivo de ameaças de malware. Às vezes os usuários desabilitam o firewall do Windows devido às notificações e pop-ups e acabam esquecendo. Se você quiser reiniciá-lo em um PC, acesse o Painel de Controle, “Sistema e Segurança” e selecione “Firewall do Windows”. Se você for um usuário do Mac, acesse “Preferências do Sistema”, “Segurança e Privacidade” e a guia “Firewall” para habilitar o recurso.

9. Utilize software antivírus.

Instale sempre a última versão do programa antivírus em seu laptop. Programas antivírus podem ajudar a proteger você durante o uso de uma rede Wi-Fi pública, detectando malwares que possam invadir seu sistema ao utilizar uma rede compartilhada. Você receberá um alerta caso vírus conhecidos sejam carregados em seu dispositivo, ou caso haja qualquer atividade suspeita, ataque ou se um malware invadir seu sistema.

10. Utilize autenticação de dois fatores ou multifator.

Utilize autenticação multifator (MFA) para fazer logon em sites da Web com suas informações pessoais. Este tipo de autenticação significa que você tem um segundo código de verificação (enviado por texto para seu celular ou fornecido por um aplicativo ou chave física) que aumenta seu nível de proteção. Assim, mesmo que um hacker obtenha seu nome de usuário e senha, ele não conseguirá acessar suas contas sem um código de autenticação.

11. Fique atento a seus dispositivos pessoais.

Não deixe seu laptop, tablet ou smartphone abandonados em um espaço público ou veículo. Mesmo que você esteja tomando precauções em uma rede Wi-Fi, não será suficiente para impedir que alguém se aposse de seus pertences ou espreite suas informações. Fique atento e vigilante quanto às pessoas ao seu redor.

12. Outras dicas de segurança online.

Leia abaixo algumas dicas para manter a segurança online, principalmente se você estiver utilizando uma conexão Wi-Fi pública:

- Utilize senhas robustas.
- Criptografia seus dispositivos.
- Fique atento a e-mails de phishing.
- Tenha cuidado com aquilo que você posta em mídias sociais. Divulgar muitos detalhes pessoais pode ajudar hackers a adivinharem senhas.
- Exclua informações antigas das quais você não precisa mais.
- Se alguma rede solicitar que você instale alguma extensão de navegador ou software adicional, não se conecte.
- Mantenha sempre as versões mais recentes de atualizações de softwares e patches em seus dispositivos para se proteger contra problemas conhecidos.