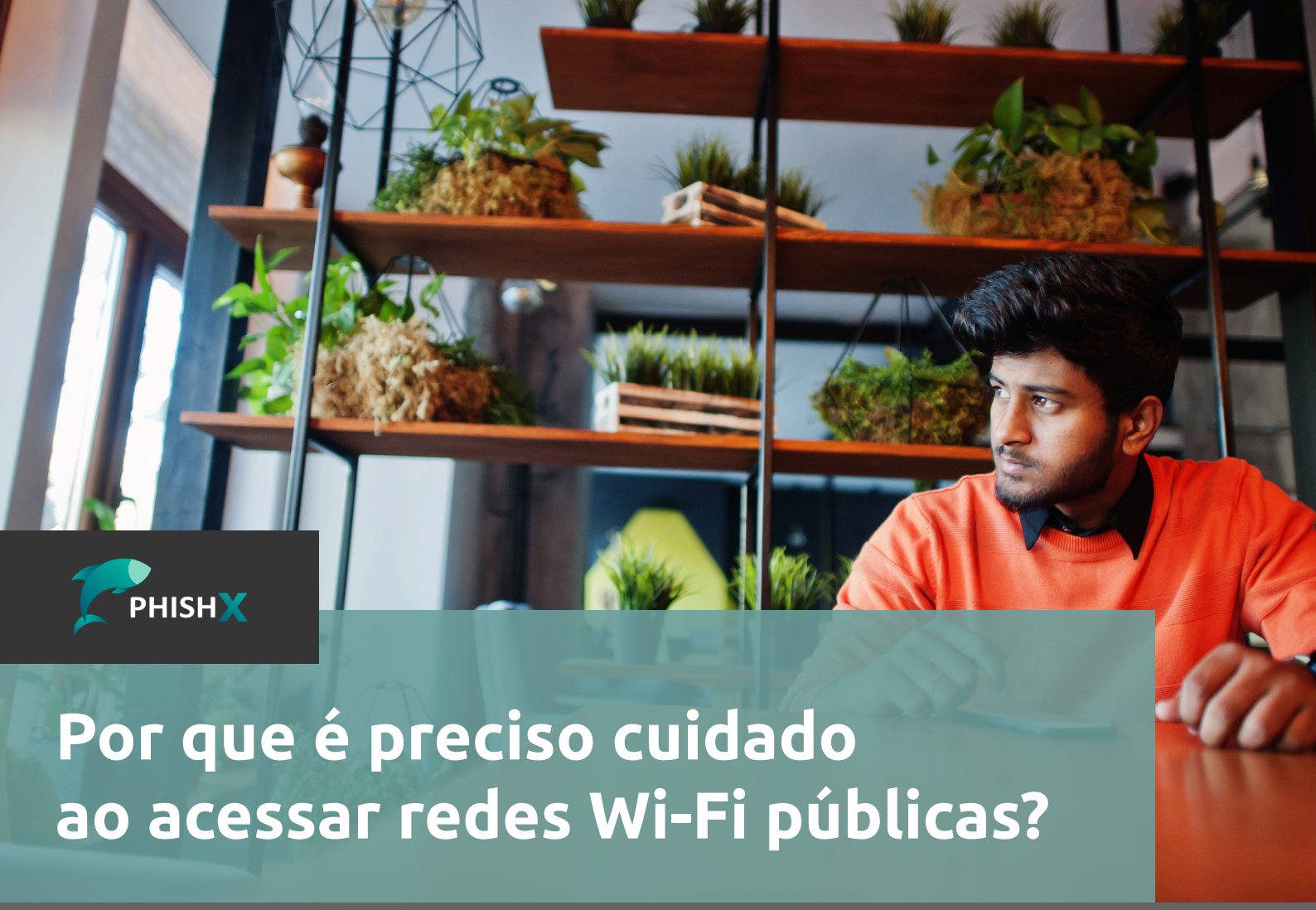

PHISHX

Por que é preciso cuidado ao acessar redes Wi-Fi públicas?

Quais são os riscos?

Apesar de úteis, redes Wi-Fi públicas podem ser um grande risco para a sua segurança digital. Por, normalmente, serem mal protegidas, elas se tornam alvo fácil para criminosos roubarem dados pessoais. Dessa forma, é melhor evitar a utilização dessas redes, porém, quando são a única opção, é preciso atenção.

Muitas vezes as redes públicas, mesmo aquelas que são protegidas por um cadastro, não contam com protocolos de segurança simples e podem ser acessadas por qualquer usuário. Isso quer dizer que não há como controlar quem as utiliza, permitindo que pessoas mal intencionadas utilizem essas vulnerabilidades para roubar informações.

Como os criminosos atuam

Entre as maiores ameaças das redes públicas, está a possibilidade de um hacker se posicionar entre o usuário e o ponto de conexão. Isso significa que um invasor pode interceptar o acesso à rede, passando a colher informações das pessoas. Enquanto está conectado, outra pessoa pode estar acessando dados que você envia pela internet, como senhas, e-mails importantes e informações de cartões de crédito.

Os criminosos também utilizam essas redes para plantar softwares maliciosos em dispositivos móveis e computadores. Por isso, é importante não permitir o compartilhamento de arquivos pela rede. É possível desabilitar a permissão nas configurações dos dispositivos.

Também é comum observar redes Wi-Fi falsas, com o mesmo nome de estabelecimentos. Elas são utilizadas para atrair vítimas para golpes cibernéticos. Para evitar acessar essas redes, procure um membro da equipe do local, ou procure placas, para confirmar qual a rede correta.

Privacidade

O usuário ainda pode enfrentar violações de privacidade mesmo em situações em que a rede Wi-Fi pública é segura contra invasores. As empresas que oferecem essas redes podem coletar informações sobre os usuários de forma indesejada. É muito comum a coleta de dados para fins de propaganda ou estatística.

Caso você esteja preocupado com o acesso aos seus dados, verifique os termos de serviço cuidadosamente antes de concordar.

Se proteja

Como vimos, a falta de ferramentas de proteção nas redes Wi-Fi públicas faz delas um grande atrativo para a prática de crimes cibernéticos. Por isso, é importante utilizá-las apenas em último caso. Porém, com algumas precauções, você pode se manter seguro enquanto utiliza as redes gratuitas.

Quando não houver alternativas, procure não acessar sua conta bancária. Evite também utilizar sites de compras e fazer login em redes sociais e contas de e-mail.

Fique atento

Desconfie sempre dessas redes, nós já vimos aqui que elas podem ser configuradas por hackers para colher suas informações. Então, sempre verifique se a rede é legítima.

Também é importante não ignorar avisos do navegador sobre certificados de segurança inválidos. Enquanto estiver conectado às redes públicas, procure acessar sites que tenham criptografia HTTPS, isso garante mais um nível de proteção.

Procure evitar fazer o download de qualquer arquivo ou sistema enquanto estiver conectado, eles podem conter vírus que vão comprometer sua privacidade.

Mantenha os dispositivos atualizados

Além disso, mantenha seus dispositivos sempre atualizados. Isso vai garantir que você evite vários ataques que se aproveitam de vulnerabilidades. Para ter um acesso mais seguro, sempre instale as últimas atualizações dos seus sistemas o mais rápido possível.

Alternativas

É muito mais seguro acessar sites que exigem e armazenam informações sigilosas, como redes sociais, bancos e sites de compra online, pela conexão de dados do celular. Assim, se você realmente precisar fazer acessar esse tipo de site, considere ampliar o seu plano de dados móveis.

Você também pode considerar o uso de uma rede privada virtual, chamada de VPN, elas mascaram os seus dados e adicionam mais uma camada de criptografia à sua conexão, garantindo um acesso seguro.