Segurança em Foco

CPSI - Comissão Permanente de Segurança da Informação
SSI - Seção de Suporte e Segurança da Informação
ASCOM - Assessoria de Comunicação Social e Cerimonial

Cuidados ao acessar UMA REDE SEM FIO

Edição nº07
Janeiro/2021

Rede sem fio (Wi-Fi) é um tipo de rede local que utiliza sinais de rádio para comunicação. Redes Wi-Fi se tornaram populares pela mobilidade que oferecem e pela facilidade de instalação e de uso em diferentes tipos de ambientes.

Embora sejam bastante convenientes, há **alguns riscos que você deve considerar ao usá-las**, como:

Por se comunicarem por meio de sinais de rádio, não há a necessidade de acesso físico a um ambiente restrito, como ocorre com as redes cabeadas. Devido a isto, os dados transmitidos por clientes legítimos podem ser interceptados por qualquer pessoa próxima com um mínimo de equipamento (por exemplo, um notebook ou tablet);

Por terem instalação bastante simples, muitas pessoas as instalam em casa (ou mesmo em empresas, sem o conhecimento dos administradores de rede), sem qualquer cuidado com configurações mínimas de segurança, e podem vir a ser abusadas por usuários maliciosos, por meio de uso não autorizado;

Em uma rede Wi-Fi pública (como as disponibilizadas em aeroportos, hotéis e conferências) os dados que não estiverem protegidos(criptografados) podem ser indevidamente lidos por usuários maliciosos;

Uma rede Wi-Fi aberta pode ser propositadamente disponibilizada por usuários maliciosos para atrair usuários, a fim de interceptar o tráfego (e coletar dados pessoais) ou desviar a navegação para sites falsos.

Diante destes riscos, podemos tomar os seguintes cuidados:

1. Conecte-se a redes públicas que sejam de sua confiança;

2. Na dúvida, é melhor utilizar o 3G/4G do seu aparelho, sempre quando possível. Se for imprescindível realizar alguma transação financeira ou acessar serviços que exijam autenticação com e-mail/usuário e senha, o recomendado é que a rede 3G/4G seja usada ao invés da conexão pública;

3. Certifique-se de que a rede Wi-Fi que está sendo acessada pelo seu dispositivo é a mesma ofertada pelo estabelecimento. Existem vários golpes em que redes paralelas são montadas para obter informações dos usuários;

4. Não execute transações financeiras como acessos a bancos, cartão de crédito, etc em redes públicas;

5. Habilite a interface de rede Wi-Fi do seu computador ou dispositivo móvel somente quando for usá-la e desabilite-a após o uso;

6. Use, quando possível, redes que oferecem autenticação e criptografia entre o cliente e o Access Point (evite conectar-se a redes abertas ou públicas, sem criptografia, especialmente as que você não conhece a origem);

7. Considere o uso de criptografia nas aplicações, como por exemplo, uso de VPNs;

8. Selecionar no Windows a opção "Público" ao se conectar pela primeira vez a uma nova rede desprotegida;

9. Evite o acesso a serviços que não utilizem conexão segura ("https");

10. Use o protocolo WPA2 sempre que disponível (caso seu dispositivo não tenha este recurso, utilize no mínimo WPA);

11. Certifique-se de fazer o logoff de qualquer serviço que tenha acessado. A seguir, acione seu aparelho para esquecer a rede. Dessa forma, ele não se conectará a ela automaticamente.

Agora que você já conhece as principais dicas, utilize-as para evitar qualquer tipo de problema. Lembre-se de que os riscos de ter outra pessoa utilizando a mesma conexão são maiores do que uma simples perda de velocidade de navegação.

Fique ligado: no próximo mês, falaremos sobre Redes Sociais!

Tribunal Regional Eleitoral - RN