SANS SECURITY AWARENESS

O boletim mensal de conscientização de segurança para você

Virtual Private Networks (Rede Privada Virtual - VPN)

Visão geral

Talvez você precise usar o Wi-Fi público para ter acesso à Internet quando estiver longe de casa, como quando está em um restaurante ou lanchonete local ou ao viajar a um hotel ou aeroporto. Mas, qual é o nível de segurança dessas redes públicas e quem está vendo ou gravando o que você está fazendo online? Talvez você não confie em seu ISP (provedor de serviços de Internet) em casa e queira ter certeza de que não podem monitorar o que você faz online. Proteja suas atividades online e privacidade com algo chamado VPN (Rede Privada Virtual - VPN). Uma VPN é uma tecnologia que cria um túnel privado e criptografado para sua atividade online, tornando muito mais difícil para qualquer pessoa ver ou monitorar o que você está fazendo online. Além disso, uma VPN ajuda a ocultar sua localização, tornando muito mais difícil para os sites acessados determinar onde você está localizado.

Como isso funciona?

Uma VPN funciona criando um encapsulamento criptografado privado para um provedor de VPN que você escolhe. Todas suas atividades online passam por esse túnel e, em seguida, saem da rede do seu provedor de VPN ao destino pretendido. Por exemplo, se você estiver em Tampa, na Flórida, e se conectar a um servidor VPN em Munique, na Alemanha, qualquer site em que você se conectar acreditará que você está se conectando de Munique, na Alemanha. Um VPN é fácil de usar. O primeiro passo é encontrar um provedor de VPN que você confie e, em depois, criar uma conta com eles (isso normalmente exige que você compre o serviço deles). Depois de ter uma conta, você baixa, instala e configura o software VPN do provedor. Uma vez instalado e configurado, você se conecta à Internet como sempre faz. O software VPN criará silenciosamente seu túnel criptografado e começará a proteger sua privacidade sem que você perceba.

Escolhendo um provedor de VPN

Suas atividades online são tão seguras e privadas quanto seu provedor de VPN. Certifique-se de escolher um confiável. Confira os pontos principais ao escolher um provedor de serviço de VPN.

Registro: procure um serviço que não mantenha registros e se concentre na privacidade. Se o seu provedor de serviços de VPN não coleta nenhum registro, é muito mais difícil para qualquer um voltar e ver o que você fez online.

Onde é a sede da empresa: Os diferentes provedores de VPN possuem sede em diferentes países. Certifique-se de selecionar um provedor de VPN com sede em um país que tenha leis de privacidade fortes. Os provedores de VPN localizados em países com pouquíssimas ou leis fracas de privacidade podem ser forçados a desistir das informações que coletam sobre você.

Servidores: procure por um serviço de VPN que tenha os servidores localizados nos países ou cidades que você precisa. Alguns provedores de VPN possuem milhares de servidores e locais em todo o mundo. Você precisa fazer com que as suas conexões apareçam como se estivessem vindo de um país específico? Seu provedor de VPN pode oferecer esse serviço?

Compatibilidade : procure serviços que funcionem em diferentes computadores e dispositivos móveis. Por exemplo, você pode usar um laptop Windows, um tablet e um iPhone. Você quer um serviço VPN que funcione em todos esses dispositivos.

Evite Grátis: Tenha muito cuidado com os serviços de VPN "gratuitos", como eles estão ganhando dinheiro e mantendo seu negócio? Serviços gratuitos podem coletar e vender suas informações.

Uma VPN é um jeito incrível de ajudá-lo a proteger sua privacidade online. No entanto, uma VPN não faz nada para proteger seu computador, dispositivos ou suas contas online. Portanto, mesmo se você estiver usando uma VPN, certifique-se de seguir sempre os passos básicos de segurança, a fim de garantir que seus dispositivos estejam atualizados, use um bloqueio de tela e sempre use senhas fortes e exclusivas para todas as suas contas.

Editor convidado

Phil Johnsey *(@peakreflections) é um profissional de TI do Condado de Palm Beach com experiência em segurança, análise forense e auditoria. Certificado no SANS em análise forense digital, essencial de segurança e membro do conselho de revisão da comunidade OUCH. Sua paixão é tornar a segurança simples para os outros.*

Recursos

Ataques Personalizados:	https://www.sans.org/u/Sd8
Protegendo seus Dispositivos Móveis:	https://www.sans.org/u/Sdd
Parar Malware:	https://www.sans.org/u/Sdi