SANS SECURITY AWARENESS

Boletín mensual de concientización en seguridad para ti

Redes Privadas Virtuales (VPN)

Resumen

Seguramente alguna vez has necesitado usar una Wi-Fi pública para acceder a Internet cuando estás fuera de casa, como en un restaurante, en una cafetería o en un hotel mientras estás de viaje o en un aeropuerto. Pero ¿qué tan seguras son estas redes y quién puede escuchar o guardar lo que estás haciendo en línea? Quizá ni siquiera confías en tu proveedor de servicios de Internet (ISP, por sus siglas en inglés, Internet Service Provider) en casa y deseas asegurarte de que no pueden monitorear lo que realizas al conectarte. En estos casos, puedes proteger tus actividades en línea y tu privacidad con algo llamado Red Privada Virtual (VPN, Virtual Private Network). Una VPN es un tipo de tecnología que crea un túnel privado y cifrado para que lo que realizas en línea sea mucho más difícil de ver o monitorear para otros. Además, una VPN ayuda a ocultar tu ubicación, haciendo mucho más difícil para los sitios que visitas, determinar dónde te encuentras.

¿Cómo trabaja una VPN?

La función de una VPN se da al crear un túnel privado y cifrado a tu proveedor de VPN. Toda tu actividad en línea viaja a través de este túnel y luego deja la red del proveedor para dirigirse desde ahí hasta su destino previsto. Por ejemplo, si te encuentras en Tampa, Florida, y te conectas a un proveedor de VPN en Munich, Alemania, cualquier sitio al que te conectes asumirá que te estás conectando desde Munich. Una VPN es fácil de usar. El primer paso es encontrar un proveedor de VPN en el que confíes y crear una cuenta con él (usualmente esto requiere realizar un pago por el servicio). Una vez que has creado tu cuenta, descargas, instalas y configuras el software de VPN que el proveedor te proporciona. Ya con la instalación y la configuración realizadas, puedes conectarte a Internet como usualmente lo haces, con lo que el software VPN creará el túnel y comenzará a proteger tu privacidad sin que te des cuenta de ello.

Seleccionando un proveedor de VPN

Tus actividades en línea se encontrarán tan seguras y privadas como lo sea tu proveedor de VPN, por lo que es importante que trates de seleccionar uno en el que puedas confiar. Aquí están algunos puntos importantes para seleccionar un proveedor de VPN:

Registro: Busca un proveedor que no mantenga registros y se enfoque en la privacidad. Si tu proveedor de VPN no guarda ningún tipo de registros, es mucho más difícil para cualquiera poder saber lo que hiciste en algún momento en línea.

Dónde se ubica la compañía: Existen proveedores de VPN que se ubican en diferentes países. Asegúrate de seleccionar uno que se encuentre en un país que tenga una legislación adecuada en temas de privacidad. Los proveedores de VPN que se encuentran en países donde no existen leyes que protejan la privacidad (o son aún muy incipientes), pueden verse forzados a entregar información que recolectan sobre ti y tu actividad.

Servidores: Busca un servicio de VPN que cuente con servidores en las ciudades o los países que son de tu interés. Algunos proveedores de VPN tienen cientos de servidores y ubicaciones alrededor del mundo. Si necesitas que tus conexiones aparenten venir de un país en específico, ¿puede tu proveedor de VPN realizar conexiones desde ese país?

Compatibilidad: Busca servicios de VPN que funcionen en diferentes computadoras y dispositivos móviles. Por ejemplo, puede que uses una laptop con Windows, una tablet y un iPhone, por lo que te recomendamos verificar que el servicio funciona en todos tus dispositivos.

Evita el uso de servicios gratuitos: Se cuidadoso cuando algo aparente ser un servicio de VPN "gratuito", pues es importante pensar en cómo es que obtienen ganancias y se mantienen en el negocio. Puede ser que estos servicios gratuitos recolecten y vendan tu información.

Una VPN es una increíble forma para proteger tu privacidad en línea, sin embargo, es importante recordar que no te ayuda a asegurar tu equipo, dispositivos o tus cuentas en línea. Por ello si usas una VPN, asegúrate de siempre seguir los consejos básicos de seguridad como mantener tus dispositivos actualizados, utilizar una clave de acceso a tu dispositivo y que estas sean fuertes y únicas para cada una de tus cuentas.

Versión en español

UNAM-CERT, Equipo de Respuesta a Incidentes de Seguridad de la Información en México reconocido ante FIRST, es una referencia en la materia en este país.
Sitio web: http://www.seguridad.unam.mx
Síguelo en Twitter @unamcert

Editor Invitado

Phil Johnsey *(@peakreflections) es un profesional de TI en el condado de Palm Beach County, con experiencia en seguridad, análisis forense y auditoría. Está certificado en forense digital y en fundamentos de seguridad por el SANS, además de ser miembro de la junta de revisión de la comunidad OUCH. Su pasión es hacer la seguridad de una manera más simple para otros.*

Recursos

Creando contraseñas simples:	https://www.sans.org/u/Sd8
Asegura tus dispositivos móviles:	https://www.sans.org/u/Sdd
Evita el malware:	https://www.sans.org/u/Sdi