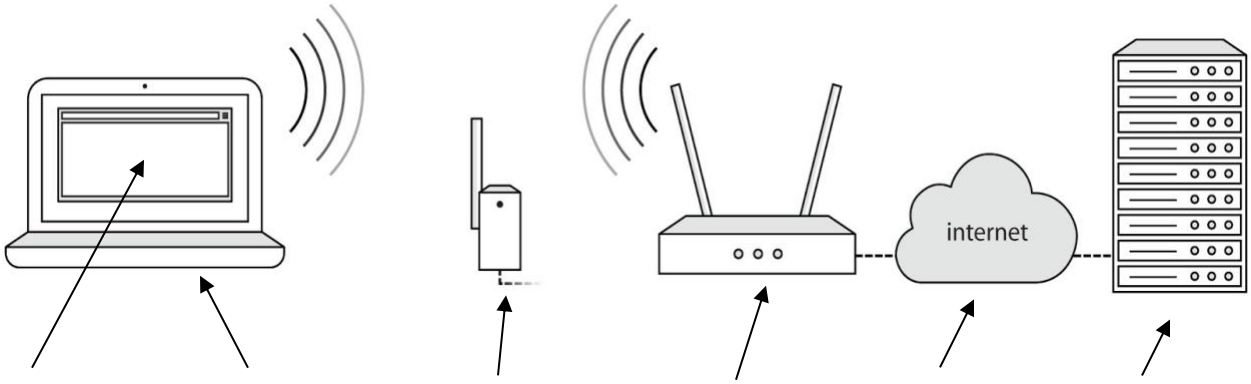
NNEDV

Seguridad y Privacidad con el WiFi: Sugerencias para Agencias de Servicios para Víctimas y Sobrevivientes

El acceso a WiFi se ha vuelto tan común que muchos lugares públicos cuentan con redes y puntos de acceso a los que usted puede conectarse. Pero, simplemente el hecho de que una red está disponible no significa que sea segura. La información a continuación les proporcionará a usted, y a los/las sobrevivientes a quienes atiende, las herramientas necesarias para mantenerse a salvo mientras utilizan cualquier red de WiFi.

Cómo Funciona el WiFi

Lo siguiente es una explicación básica de los varios pasos de la comunicación por WiFi:



Navegador
Su navegador es software que le permite ver y enviar información por internet.

Aparato
Su aparato utiliza su conexión de WiFi para transmitir información al y del navegador.

Aparato de Escuchar
Los datos que transmite se envían por el aire. Cualquier persona en el área que sabe la contraseña de WiFi puede interceptarlos.

Enrutador Inalámbrico
El enrutador recibe la comunicación de WiFi de su aparato y envía información al y del internet.

Internet
El Internet es un sistema de redes de computadoras que los aparatos utilizan para conectarse.

Destino
La información llega a los servidores de anfitrión del sitio web que visita y esos servidores le devuelven la información que usted pidió.

Los Puntos Calientes de WiFi que Usted Controla

Un punto caliente de WiFi o "Hotspot" en inglés usted puede controlar tiene la posibilidad de ser tan seguro como una conexión con cable. Para lograr este nivel de seguridad, hay que tomar los siguientes pasos:

1. Utilizar una Contraseña Fuerte y Privada

Elija una contraseña de WiFi que sea larga. Las mejores contraseñas tienen, como mínimo, de 12 a 15 caracteres y contienen letras, números y símbolos colocados de manera aleatoria. Lea más sobre Seguridad de las contraseñas. No reparta esta contraseña ni la escriba en ningún lugar visible (incluyendo en o cerca del punto caliente mismo).

2. Cambiar los Ajustes de Seguridad

La configuración apropiada asegurará que su Punto Caliente de WiFi sólo apoye los protocolos más actualizados para transmitir información:

- El único algoritmo que debe estar activado es WPA2. Desactive WEP y WPA.
- El único método de encriptación que debe estar activado es AES. Desactive cualquier ajuste relacionado a TKIP.
- Desactive WPS por completo. Este servicio está activado por defecto en la mayoría de los Puntos Calientes. Permite otro método de conectarse sin contraseña. Tiene un defecto de seguridad significativo que es fácil de explotar.

3. Establecer una Red de Invitados/as *(opcional)*

Establezca una red alternativa si tiene invitados/as que necesitan acceso a su conexión de internet. La contraseña para esta red no tiene que ser tan compleja ni privada. El nombre para la red no debería ser identificable, por su privacidad y para sus invitados.

Los pasos para tener acceso a y configurar un Punto Caliente de WiFi son diferentes para cada aparato. Es posible que necesite la ayuda de alguien con experiencia para hacer estos cambios.

Puntos Calientes de WiFi Abiertos/Públicos

Si tiene preocupaciones o riesgos graves de privacidad, es crítico entender cómo utilizar una red de WiFi pública/abierta seguramente y cuando es mejor evitarla. Se debe considerar cualquier Punto Caliente de WiFi donde no haya contraseña o la contraseña esté disponible al público como una red abierta (un típico ejemplo

de esto es en un hotel donde todos los huéspedes tienen la misma contraseña y no se modifica con frecuencia). Incluso si la red tiene protección de contraseña, alguien con conocimientos de cómo escuchar a escondidas todavía podrá ver sus comunicaciones si también tiene acceso a la contraseña.

Hay dos maneras en que se puede navegar el internet seguramente al utilizar un Punto Caliente de WiFi público:

1. Utilizar HTTPS

HTTPS añade un nivel casi impenetrable de encriptación entre su navegador y el sitio web con el que comunica. ***Sí*** se puede confiar en los sitios que utilizan una conexión HTTPS, incluso al utilizar una red de WiFi abierta/pública. Pero, siempre debe comprobar que hay "https" al principio de la dirección de web y verificar que el nombre de dominio es exactamente el sitio que usted quiere. Guardar los sitios web importantes como marcadores y siempre ir a esos sitios web utilizando esos marcadores es una excelente manera de asegurarse de no ser engañado/a e ir a un sitio que no es lo que parece ser. Siempre se debe prestar atención a los avisos que su navegador le da sobre problemas con el certificado de seguridad de un sitio web con HTTPS.

También es importante recordar que mientras el ***contenido*** de sus comunicaciones con HTTPS sea privado, el ***destino*** no lo es. Imagine que le ha enviado una carta por correo a un/a amigo/a utilizando un idioma que sólo ustedes entienden pero la dirección en el sobre está escrita en un idioma que todo el mundo entiende. Cualquier persona que intercepte esa carta *no* podrá leer el mensaje adentro pero *sí* podrá ver con quien está comunicando al leer el sobre. El mismo concepto aplica a las comunicaciones de la red.

Las actividades que generalmente son seguras al utilizar HTTPS:

La dirección de web o el destino típicamente no es un secreto; pero, se puede confiar en HTTPS para proteger el contenido de:

- Transacciones bancarias o compras en línea
- El email basado en la red (Gmail, Yahoo! Mail, etc.)

- Las redes sociales (Facebook, Instagram, etc.)
- Cualquier otro servicio de la red que requiere un nombre de usuario/a y contraseña para ver la información

Las Actividades que NO son privadas con HTTPS:
La información en la dirección de web (el destino) revela la información leída

- Los motores de búsqueda (Google, Bing, etc.)
- Los mapas en línea (Mapas de Google, MapQuest, etc.)
- Cualquier sitio web que no quisiera que alguien que escuchaba a escondidas supiera que ha visitado

La línea entre el "contenido" y el "destino" de un sitio web puede ser vaga. Si tiene dudas, siempre presuma que su información no es privada. Espere hasta que tenga una conexión de internet que usted controla antes de seguir.

2. Utilizar una Red Privada Virtual (VPN por sus siglas en inglés)
Una manera fácil de evitar casi todos los riesgos para la privacidad relacionados al WiFi es tener una suscripción para una red privada virtual (VPN). Una VPN cifrará el 100% del tráfico que su computadora envía y lo entregará a un servidor alternativo en otro lugar en el internet. Una vez que la información haya llegado al servidor alternativo, se descifrará y se enviará a su último destino. La VPN hace que parezca que las peticiones que usted envió vinieron de ese servidor alternativo y mantenga anónimas su dirección de IP y ubicación.

Una VPN proporciona los siguientes beneficios:

- Cifra todo el tráfico de la red (HTTP y HTTPS) mientras viaja por WiFi
- Enmascara ambos el contenido de la red **y** el destino mientras viaja por WiFi
- Enmascara su dirección de IP original del sitio web que visita. Esto previene que el sitio web siga su dirección de IP hasta su área geográfica.

Otras Sugerencias de Seguridad

1. Mantener Actualizado el Software

Es importantísimo que actualice pronto su sistema operativo, su navegador, su programa de anti-virus y cualquier otra cosa en su computadora, tableta o aparato relacionado al internet o a la seguridad. Si no los actualice, su computadora será vulnerable. Siempre se descubren nuevas amenazas y estas actualizaciones ayudan a proteger contra esas amenazas pero sólo cuando sean las versiones más recientes. Puede ser útil pensar en las actualizaciones como un techo con agujero - si no lo arregla tan pronto como sea posible, las cosas podrían convertirse en algo muy grave pronto y su techo podría hundirse.

2. Utilizar Software de Anti-Virus/Anti-Programas Espía

Aunque no son perfectos, los programas anti-virus/anti-programas espía todavía son una herramienta importante para parar el contenido malicioso antes que pueda llegar a su navegador.

La mayoría de las computadoras ya tienen instaladas aplicaciones de anti-malware y anti-programas espía. Estas aplicaciones típicamente sólo son gratuitas por un período inicial y no se debe depender de estas aplicaciones después de la fecha de vencimiento. También se puede descargar una variedad de programas gratuitos de anti-virus.

Hay aplicaciones anti-malware disponibles para celulares pero no proporcionan tantos beneficios como las que hay para computadoras.

Es importante evaluar por completo cualquier programa de anti-virus antes de instalarlo. Es común que los programas de malware se disfracen como programas de anti-virus o herramientas para escanear su computadora para engañarle para que los instale.

3. Utilizar Pantallas de Privacidad

Una manera de baja tecnología de prevenir que alguien mire por encima de su hombro para ver la información en sus aparatos es utilizar una pantalla de

privacidad. Las pantallas de privacidad son filtros oscuros para poner encima de la pantalla de su portátil o tableta para prevenir que alguien vea lo que usted está haciendo.

4. Administre el historial de la red de WiFi

La mayoría de los dispositivos móviles y computadoras almacenan una lista de las redes de WiFi a las que se ha conectado. Revise la lista y elimine todas las que no sea seguro guardar. Es posible que no quiera borrar la lista completa porque eso podría levantar sospechas en alguien que controla físicamente sus dispositivos. Además, podría no ser conveniente borrar la lista completa porque, probablemente, allí se encuentra la red de WiFi a la que usted se conecta con mayor frecuencia (incluidas las contraseñas).

Lo Que Los/Las Sobrevivientes e Intercesores/as Pueden Hacer

Para víctimas de violencia doméstica, acecho y agresión sexual y sus intercesores/as, hay algunas opciones adicionales para aumentar su seguridad.

1. Hacer Planes de Seguridad

Para sobrevivientes del abuso, tener acceso seguro al internet es importante. Es importante hacer planes de seguridad sobre el uso de tecnología y actualizar esos planes con regularidad. Comparta esta información sobre la seguridad con las redes de WiFi con sobrevivientes para que puedan tomar decisiones informadas en cuanto a su uso del internet.

2. Conocer sus Aparatos

La mayoría de los aparatos tienen ajustes que aumentan la seguridad. Ambos los/las intercesores/as y los/las sobrevivientes deben saber cómo cambiar, modificar y desactivar los ajustes en sus aparatos. Para más información sobre los varios ajustes y capacidades para aparatos, visite TechSafety.org.

3. Confíe en sus Instintos

Siempre confíe en sus instintos. Si piensa que una red, un sitio web o un servicio particular no es fiable, tenga cuidado al utilizarlo. Si necesita utilizarlo, no comparta información confidencial mientras lo hace.

Para Resumir

El internet es una herramienta maravillosa y los/las sobrevivientes tienen el derecho de conseguir acceso a información libremente sin tener miedo por su seguridad. Es una herramienta importante que les permite a sobrevivientes sentirse empoderados/as e independientes. Pero, los/las sobrevivientes e intercesores deben estar conscientes de los riesgos y saber cómo manejarlos. Con estas sugerencias y estrategias, ambos/as los/las sobrevivientes e intercesores/as pueden reducir la vulnerabilidad de sus aparatos y el riesgo de que sus aparatos y su información sean comprometidos al utilizar cualquier red de WiFi.

Les agradecemos especialmente a Steven Jenkins de EmpowerDB por proporcionar conocimiento sobre este contenido.

 Apoyado por Subvención# 2013-TA-AX-K006 de DOJ-OVW de los EE.UU. Las opiniones y conclusiones o recomendaciones expresadas son de los/las autores/as y no reflejan necesariamente las de DOJ.

Actualizamos nuestros materiales con frecuencia. Por favor, visite TechSafety.org para la versión más reciente de esto y otros materiales.