Título: Consejos para Mantenerse Seguro en Línea: Cómo Usar una Wi-Fi Pública

Presentación: La Serie de Videos Consejos para Mantenerse Seguro en Línea se organiza mediante diapositivas como marcadores visuales. Cualquier imagen de las diapositivas que sea importante para el contenido, y exprese cualquier información adicional más allá del guion, se incluye aquí como texto alternativo.

Narrador: Bienvenidos al video de Help@Hand Consejos para Mantenerse Seguro en Línea: Parte 2: Video sobre Cómo Usar una Wi-Fi Pública. Help@Hand es una Colaboración de múltiples ciudades y condados creada para ayudar a dar forma al futuro de soluciones de salud mental basadas en la tecnología y conectar a las personas con los cuidados por todo el estado. La intención de estos tutoriales en video es empoderar a las comunidades de California para que tomen decisiones informadas sobre la forma en que interactúan con la tecnología.

Narrador: Este es el Curso 4 de una serie de 4 cursos llamada Consejos para Mantenerse Seguro en Línea Parte 2. Los videos de esta serie pueden verse por orden, o en cualquier orden según sus intereses. En este video hablaremos de estrategias para usar redes Wi-Fi públicas para proteger sus datos personales.

Narrador: Wi-Fi es el nombre de las redes inalámbricas que nos ayudan a conectarnos a Internet sin usar cables. Podemos tener Wi-Fi en nuestros hogares y también podemos acceder a redes públicas gratuitas que se conocen como puntos de acceso Wi-Fi. Usted puede encontrar estos puntos de acceso, o “hotspots”, en lugares como la biblioteca, cafeterías, hoteles y aeropuertos.

Narrador: A pesar de que sin duda es cómodo tener acceso a Wi-Fi cuando usted está fuera de casa, es importante saber que la mayoría de los puntos de acceso Wi-Fi no tienen en funcionamiento grandes protecciones de seguridad. Al usar una red no segura, usted puede hacerse más vulnerable a extraños que podrían querer acceder a sus datos personales. A este tipo de personas se les llama “hackers”, y tienen herramientas que les pueden permitir ver sus documentos privados, sus contactos y credenciales de conexión. Si tienen esta información, pueden hacerse pasar por usted y engañar a personas de su lista de contactos. También pueden acceder a sus cuentas en línea, incluyendo aquellas que contienen información financiera.

Imagen: Se muestra una pregunta que dice, “¿Cuáles son algunas cosas que puedo hacer para protegerme mientras uso una Wi-Fi pública?”

Narrador: A pesar de que lo más seguro siempre es utilizar una conexión Wi-Fi segura en casa, hay algunas medidas que puede tomar para protegerse cuando use una Wi-Fi pública. Usted puede tener cuidado con lo que decide hacer en línea y también tomar medidas para proteger su computadora contra cualquier posible ciberataque.

Narrador: Algunas redes inalámbricas son más seguras que otras. Cuando sea posible, debe conectarse a un Acceso Protegido a Wi-Fi, llamado redes WPA y WPA2. WPA y WPA2 son herramientas de encriptado, lo cual significa que encriptan la conexión a red, de forma que nadie puede escuchar ni mirar los sitios web que usted está visitando. De los dos tipos de redes, WPA2 por lo general es más segura, y los dos tipos necesitarán una contraseña para conectarse.

Imagen: Se muestra una ventana emergente que dice “La red Wi-Fi “admin2” necesita una contraseña WPA2.” Esta ventana tiene un recuadro de texto para introducir una contraseña y dos recuadros para marcar que dicen “Mostrar Contraseña” y “Recordar esta red”; bajo estos hay dos botones en los que se puede hacer clic, un botón de “Cancelar” y un botón de “Conectar”.

Narrador: Este es un ejemplo: cuando usted selecciona una red Wi-Fi de las opciones de redes disponibles, se le pedirá que introduzca una contraseña. Si usted está en una cafetería o biblioteca o cualquier otro lugar de negocio, a menudo tendrán una contraseña para la red.

Narrador: Otra estrategia cuando se acceda a una Wi-Fi pública es navegar por sitios que tengan instaladas protecciones de seguridad. Además de utilizar una red segura, usar sitios web que hayan tomado algunas medidas para protegerle hará más difícil a los hackers robar su información.

Narrador: Este es un resumen de algunas estrategias que usted puede utilizar cuando esté considerando visitar una página web. Se puede saber mucho a partir de la dirección del sitio web, también conocida como la URL. Busque un candado y una s después de “http” y compruebe dos veces que la dirección del sitio web está escrita correctamente. Si un sitio web no cumple estos criterios, considere evitarlo cuando utilice una Wi-Fi pública, y como mínimo no introduzca ningún dato personal. Para más detalles sobre el uso de sitios seguros, vea nuestro webinario de Help@Hand de nuestra primera serie, llamado “Consulta Más Segura de Sitios Web”.

Narrador: Cuando sea posible, intente hacer su compras y operaciones bancarias en línea desde redes seguras.

Narrador: Si usa una red o sitio web no seguro, un hacker podría acceder a los datos de su tarjeta de crédito cuando usted está haciendo una compra en línea.

Narrador: Y es todavía más importante evitar realizar operaciones bancarias en línea cuando use una red no segura, porque un hacker podría acceder a los datos de su cuenta bancaria.

Narrador: Cuando use cuentas en línea, como correo electrónico o Facebook, a menudo es fácil seguir conectado; sin embargo, esto nos hace más vulnerables a los hackers.

Narrador: Como práctica general, es mejor cerrar sesión en las cuentas después de que haya acabado de utilizarlas. También puede tomar medidas para proteger sus computadoras contra ciberataques cuando esté usando una Wi-Fi pública. Una forma fácil de incrementar su nivel de protección es mantener actualizado el software de su computadora.

Narrador: Actualizar el software de su computadora significa que su computadora tendrá las protecciones de seguridad más recientes destinadas a impedir a los virus dañar su computadora. Los ciberdelincuentes están constantemente cambiando de estrategia para acceder a los datos de las personas, y por eso es importante que tenga el software más reciente instalado para ayudar a protegerle contra estas nuevas amenazas.

Narrador: Además de actualizar el software de su computadora, también puede ir un paso más allá descargando programas de software antivirus y antimalware.

Narrador: Los programas de software antivirus pueden proteger contra algunos de los virus más antiguos más comunes y el software antimalware protege contra algunas de las amenazas más recientes. Vea el webinario de Help@Hand “Cómo Descargar Programas Antivirus y Anti-Malware” para más información.

Narrador: Y finalmente, otro consejo es activar siempre el “cortafuegos” de su computadora para bloquear intentos por parte de extraños de destruir datos de su computadora.

Narrador: Su cortafuegos se interpone entre su computadora e internet. Su propósito es servir de escudo contra hackers que estén intentando acceder a datos de su computadora.

Narrador: Normalmente podrá encontrar esta configuración dentro de las “preferencias de sistema” de su computadora.

Narrador: Para proteger sus datos personales, es importante no olvidar estas estrategias cuando use una Wi-Fi pública. Cuando sea posible, use una red segura, visite sitios que apliquen protecciones de seguridad, limite las compras y las operaciones bancarias en línea y cierre sesión en sus cuentas cuando no esté utilizándolas.

Narrador: También puede tomar medidas para proteger su computadora actualizando regularmente sus programas, instalando protección antivirus y antimalware y activando el cortafuegos de su computadora. Vea el video de Help@Hand sobre Cómo Descargar Programas Antivirus y Anti-Malware para más información.

Narrador: Esperamos que haya encontrado útil este vídeo. A pesar de que es opcional, le rogamos que, por favor, dedique un minuto a proporcionar retroinformación sobre su experiencia, haciendo clic en el enlace de encuesta que aparecerá en breve. Gracias por participar, y no olvide ver los demás videos de Help@Hand