Consejos de seguridad informática para viajeros internacionales

Al viajar al extranjero, recuerde que su teléfono móvil y otros dispositivos de comunicaciones personales transmiten y almacenan su información personal, que es tan valiosa como el contenido de su maleta, o quizás más.

Antes de irse

Tome medidas proactivas para proteger sus dispositivos y su información de identificación personal antes de viajar. Deje en casa los equipos electrónicos que no necesitará durante el viaje y, si los lleva, protéjalos. Asegúrese de hacer lo siguiente:

- Realizar una copia de seguridad de sus archivos electrónicos.
- Eliminar los datos confidenciales.
- Establecer contraseñas seguras.
- Asegurarse de que el software antivirus esté actualizado.

Durante el viaje

Esté atento a dónde y cómo usa sus dispositivos, y no se confíe demasiado. Asegúrese de hacer lo siguiente:

- Proteja sus dispositivos en lugares públicos, como aeropuertos, hoteles y restaurantes.
- Preste atención a su alrededor y tenga cuidado de que nadie esté mirando la pantalla de su dispositivo cuando lo usa para intentar robarle información.
- Considere usar una pantalla de privacidad en su computadora portátil.

Tenga cuidado al usar wifi público.

Algunas amenazas (por ejemplo, el robo de dispositivos) son evidentes, pero otras pueden ser invisibles, como los ladrones de datos que intentan descifrar contraseñas para poner en peligro su información de identificación personal o acceder a sus cuentas. Usted puede ser especialmente vulnerable en lugares que tienen wifi público, incluidos los cibercafés, las cafeterías, las librerías, las agencias de viaje, las clínicas, las bibliotecas, los aeropuertos y los hoteles. Algunos consejos útiles:

- No use las mismas contraseñas o números de PIN en el extranjero que usa en los Estados Unidos.
- No use el wifi público para realizar compras en línea o acceder a las cuentas bancarias.
- Al conectarse a una red pública, desactive la función de entrada automática de su teléfono.
- Al usar una red wifi pública, ajuste periódicamente la configuración de su teléfono para que olvide la red y conéctese nuevamente.
- Intente conectarse intencionadamente al wifi público con una contraseña incorrecta. Si se puede conectar, es una señal de que la red no es segura.

Federal Communications Commission · Consumer and Governmental Affairs Bureau · 445 12th St. SW. Washington, DC 20554
1-888-CALL-FCC (1-888-225-5322) · TTY: 1-888-TELL-FCC (1-888-835-5322) · Fax: 1-866-418-0232 · www.fcc.gov/espanol

También recuerde evitar el uso de equipos públicos, como teléfonos, computadoras y máquinas de fax, para comunicaciones confidenciales.

Al llegar a su casa

Los dispositivos y aparatos electrónicos utilizados u obtenidos en el extranjero pueden verse afectados. Su teléfono móvil y otros dispositivos electrónicos pueden ser vulnerables al malware si se conecta a redes locales en el extranjero. Actualice su software de seguridad y cambie sus contraseñas en todos los dispositivos al regresar a su casa.

Recursos adicionales

Para obtener más consejos, consulte la página web del Equipo de Respuesta ante Emergencias Informáticas (www.us-cert.gov/cas/tips) del Departamento de Seguridad Nacional (en inglés).

Las leyes y políticas sobre la seguridad y privacidad en línea son diferentes en otros países. Cuando se encuentre en un país extranjero, estará sujeto a las leyes locales. El sitio web del Departamento de Estado contiene información de seguridad de viaje (http://travel.state.gov/content/passports/english/country.html) (en inglés) para todos los países del mundo.

Otros formatos

Para solicitar este artículo en formato accesible - Braille, letra grande, Word o documento de texto o de audio - escríbanos o llámenos a la dirección o teléfonos de más arriba o envíenos un correo electrónico a fcc504@fcc.gov.

Última edición: 18 de julio de 2018

Federal Communications Commission · Consumer and Governmental Affairs Bureau · 445 12th St. SW. Washington, DC 20554
1-888-CALL-FCC (1-888-225-5322) · TTY: 1-888-TELL-FCC (1-888-835-5322) · Fax: 1-866-418-0232 · www.fcc.gov/espanol