Protección para los Servicios de Billeteras Móviles

Numerosos consumidores usan sus teléfonos inteligentes, sus tabletas electrónicas y otros aparatos inalámbricos como “billeteras móviles” --para pagar por bienes y servicios, utilizando programas computacionales (*software* en inglés) destinados a efectuar transacciones móviles y en persona. A medida que el uso de los servicios prestados vía billeteras móviles aumenta, tambien aumenta la necesidad de proteger --de robos y de ataques cibernéticos-- sus teléfonos inteligentes, sus aplicaciones para billeteras móviles y la información asociada a estas últimas.

Cómo resguardar su billetera móvil

- Nunca deje su teléfono inteligente descuidado, en un lugar público o visible en un auto sin ocupantes.
- Esté consciente de su entorno y use su teléfono inteligente y su aparato móvil de manera discreta.
- Nunca use los servicios de billetera móvil mediante una red de conexión inalámbrica a Internet (*Wi-Fi* en inglés) que no cuente con resguardos de seguridad cibernética. Vea nuestra guía www.fcc.gov/consumers/guides/datos-para-resguardar-su-“bluetooth”-y-otras-conexiones-inalámbricas.
- Elija claves de ingreso exclusivas para todas las aplicaciones (*apps*).
- Instale y mantenga programas computacionales (*software,* en inglés) de seguridad. Hay aplicaciones (*apps*, por su abreviación en inglés) para:
  - Localizar su teléfono inteligente desde cualquier computadora.
  - Restringir acceso al uso de su teléfono inteligente.
  - Eliminar su información personal confidencial y las credenciales de su billetera móvil contenidas en su teléfono inteligente.
  - Generar la emisión de un intenso sonido (en forma de grito) en su teléfono inteligente para ayudarle – y a la policía-- a localizarlo.
- Tenga cuidado con las *apps* para los sitios de interacción social en Internet. Podrían representar un peligro para su seguridad y dar acceso indeseado a otras personas a su información personal y a la información de su billetera móvil.
- Vigile sus cuentas bancarias conectadas en *apps* móviles. Examine el contrato de servicios de la cuenta financiera que utiliza en su billetera móvil para averiguar qué ocurriría y a quién debe contactar en caso de que su teléfono inteligente sea robado o se haya extraviado o si la aplicación electrónica para su billetera móvil es presa de piratas cibernéticos (*hacked,* en inglés).
- Si su teléfono inteligente es hurtado o extraviado, es posible que la policía necesite la identificación única del aparato. Anote el número de modelo, el número de serie y el número de identificación única del teléfono, ya sea la identificación internacional para equipos móviles (*International Mobile Equipment Identifier, IMEI* por sus siglas en inglés) o el número identificador de equipos móviles (*Mobile Equipment Identifier, MEID* por sus siglas en inglés). Algunos teléfonos exhiben el número IMEI/MEID al marcar *#06#. También puede encontrar la identificación IMEI/MEID en una etiqueta ubicada en la parte posterior de la batería del teléfono o impresa en la caja de empaquetado del mismo.

Federal Communications Commission · Consumer and Governmental Affairs Bureau · 45 L Street NE, 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

Qué hacer si le roban su teléfono inteligente

- Si no está seguro de que su teléfono inteligente o aparato móvil ha sido robado o si simplemente lo ha extraviado, trate de localizarlo llamando a su número o usando el software de seguridad de GPS para localización.
- Si ha instalado software de seguridad en su teléfono inteligente, úselo para bloquearlo, elimine su información personal confidencial y/o active la alarma.
- Dé aviso inmediatamente a su proveedor de servicios inalámbricos en caso de robo o extravío de su aparato móvil. Si usted proporciona a su proveedor el número IMEI o MEID, éste podría estar capacitado para desactivar su teléfono inteligente, sus servicios de billetera móvil y también para bloquear el acceso a su información personal y a la información confidencial de su billetera móvil. Pida una confirmación por escrito a su proveedor de servicios inalámbricos respecto a que dio aviso del extravío de su teléfono inteligente y que éste fue desactivado.
- En caso de robo del aparato móvil, informe inmediatamente del hurto a la policía, incluyendo los números de serie de fabricación y modelo, así como los números IMEI o MEID. Algunos proveedores de servicios inalámbricos exigen prueba de que el teléfono inteligente fue robado. Un informe de la policía puede proporcionar dicha documentación.
- Si usted no puede bloquear su teléfono inteligente robado o extraviado, cambie todas las claves de ingreso de sus servicios de billetera móvil y de las cuentas bancarias a las que haya accedido usando los servicios de su teléfono inteligente.

Para obtener más información sobre qué hacer en caso de que su aparato móvil haya sido robado o extraviado y para conseguir la información de contacto de los proveedores de servicios inalámbricos, ingrese a: www.fcc.gov/consumers/guides/proteja-su-telefono-inteligente.

Presentación de quejas

Visite nuestro Centro de quejas del Consumidor https://consumercomplaints.fcc.gov (en inglés) para presentar una queja o contarnos su problema.

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 del pie de página o envíenos un correo electrónico a fcc504@fcc.gov.

Última edición: 13 de diciembre de 2017

Federal Communications Commission · Consumer and Governmental Affairs Bureau · 45 L Street NE, 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