Introducción

La Banca Móvil es un servicio basado en Internet que le permite a usted realizar operaciones bancarias de manera segura y conveniente a través de equipos móviles. Sin embargo, el uso inadecuado de los equipos móviles representa algunos riesgos de inseguridad con el fin de obtener información personal.

En la actualidad la tendencia de ataques a este tipo de servicio, tiene que ver con el robo de información, robo de identidad a través de ingeniería social y ataques de malware malicioso (virus) el cual podría llegar dañar el equipo móvil.

En esta sección encontrará información de seguridad, que le será de mucha ayuda para que pueda hacer uso de la Banca Móvil y reducir los riesgos ó amenazas a los que se está expuesto.

1. Bloquee su teléfono mediante una contraseña.

• Configure su teléfono para que se bloquee de forma automática tras un periodo de tiempo, con el fin de impedir el acceso no autorizado.
• Genere una contraseña ó patrón de desbloqueo de forma robusta si el dispositivo se lo permite.

2. Instale solamente aplicaciones desarrolladas por fuentes de confianza.

• Compre ó baje aplicaciones desde sitios de confianza. Antes de descargar una aplicación, infórmese sobre ella y sobre su editor.
• Compruebe los comentarios y las calificaciones de otros usuarios para asegurarse que la aplicación no representa ningún peligro.
• Lea la política de privacidad de la aplicación (si cuenta con ella), con el fin de conocer la información a la que tiene acceso y si la aplicación compartirá sus datos con terceros.
• Evite prestar su teléfono a personas desconocidas, ya que corre el riesgo que le sea instalado un programa malicioso y hagan uso de su dispositivo de forma malintencionada.
• Evite accesar a enlaces enviados a través de mensajes de dos vías (SMS/MMS) los cuales impliquen una descarga de contenidos en su dispositivo móvil.

3. Realice copias de seguridad de sus datos.

• Genere copias de seguridad de su información personal (contactos, fotografías, notas, documentos, etc.), con el fin de poder restaurar la misma, en caso de sufrir algún tipo de ataque físico, lógico, por la eliminación accidental de los datos o por la pérdida del dispositivo.

4. Mantenga su sistema Actualizado.

• Descargue las actualizaciones de software para el sistema operativo de su dispositivo móvil cuando se le solicite. De esta manera, siempre dispondrá de las últimas

actualizaciones de seguridad y del buen funcionamiento del dispositivo.

5. Operación Banca Móvil

• Utilice contraseñas seguras para ingresar a las aplicaciones móviles, le recomendamos que esta contraseña no contenga datos personales (fecha de nacimiento, teléfono, nombre, etc).
• Evite prestar su teléfono a personas que no conozca, ya que puede correr riesgo de alguna instalación de código malicioso (virus) con el propósito de robo de su información.
• Siempre que digite su clave, hágalo con precaución; si sospecha que alguien la conoce, cámbiela inmediatamente.
• Por seguridad, la clave que esta digitando en su acceso al aplicativo, no aparecerá en la pantalla de su dispositivo móvil.
• La aplicación tiene habilitado el manejo de inactividad, esto quiere decir si en 5 minutos de inactividad, el usuario no realizara alguna operación, la aplicación se cerrera de forma automática.

6. Desactive la WiFi, servicios de geolocalización y bluetooth cuando no los utilice.

• Desactive la conexión Wi-Fi si no la está utilizando. Los ciberdelincuentes y los ladrones de identidad pueden acceder fácilmente a su información sin que se percate de ello si la conexión no es segura. Cuando no esté conectado a su red doméstica o a la red de su empresa, utilice en su lugar una conexión de datos 3G o 4G, ya que la mayoría de los proveedores de celulares cifran el tráfico entre las torres celulares y los terminales.
• Desactive las aplicaciones que utilizan servicios de geolocalización. Es posible que lo desconozca, pero algunas empresas almacenan está información y pueden compartirla, filtrarla o utilizarla para enviarle publicidad.
• Desactive la conexión Bluetooth cuando no la necesite. Muchos dispositivos vienen por default habilitadas, que permite que otros usuarios se conecten a su dispositivo, en ocasiones sin su conocimiento. Esto significa que usuarios malintencionados podrían acceder a su dispositivo y copiar archivos u obtener acceso a otro dispositivo conectado a su dispositivo Bluetooth.

7. Reporte cualquier anomalía.

• Recuerde que por ningún medio (email, sms, red social, telefónicamente) CIBanco S.A., le solicitara sus claves de acceso (usuario y password) ni que sincronice su Token de Seguridad, si recibe este tipo de solicitudes, repórtelo inmediatamente a CIDIRECTO, en zona Metropolitana al 1103 1220 y del interior de la República al 01800 2524 226.