SEGURIDAD PARA APLICACIONES MÓVILES

Manual de recomendaciones para la Seguridad de nuestro terminal Móvil

Web: seguridadparaaplicaciones.com

13 GRANDES CONSEJOS PARA LA SEGURIDAD DE TU TELEFONO MOVIL O CELULAR

1.- Poner una contraseña en el teléfono y cambiar el PIN de la tarjeta SIM. No confíe en los ajustes de fábrica por defecto. Usando una contraseña y cambiando el PIN de su tarjeta, detendrá a los ladrones conseguir acceso a su teléfono y evitará que utilicen la tarjeta SIM en otro teléfono para hacer llamadas. Todos los teléfonos tienen configuración de seguridad para hacerles prácticamente inaccesibles sin su consentimiento.

consejos-seguridad-en-tu-movil

2.- Configure su dispositivo para que se bloquee automáticamente. Si el teléfono no se ha utilizado durante unos minutos, se debe bloquear automáticamente y requieren una contraseña o PIN para reactivarlo de nuevo.

3.- Cifre sus datos. Algunos teléfonos le permiten encriptar sus datos y si no, puede optar por un software que lo instale y lo haga. Esto es muy importante sobre todo cuando envía datos desde su terminal.

4.- Considere la instalación de software de seguridad de un proveedor de confianza. Anti-virus, anti-robo, anti-malware y firewall, son aplicaciones que no deberían faltan en su teléfono móvil o celular.

5.- Instala solo software y aplicaciones móviles (apps) de sitios web de confianza . Siempre manténgase atento a las direcciones de sus sitios web de uso común y asegúrese de que no es dirigido o desviado a otros sitios web que no son de confianza. Y sobre todo, preste mucha atención al usar cualquier aplicación móvil relativo al dinero como la banca electrónica móvil. En estos casos asegúrese de utilizar solamente las aplicaciones suministradas por la entidad financiera.

6.- Tenga cuidado al permitir aplicaciones sin certificar de terceros para acceder a su información personal. Esto incluye el acceso a su ubicación. Lea siempre las solicitudes de permiso antes de instalar nuevas aplicaciones o actualizaciones de aplicaciones, en busca de solicitudes inusuales o peticiones de dinero.


consejos-seguridad-en-tu-movil

7.- No haga clic en enlaces no solicitados o inesperados. Incluso cuando parecen ser de amigos.

8.- Revise su factura de teléfono para los cargos de datos inusuales o llamadas de tarificación adicional. Póngase en contacto con su proveedor de servicio inmediatamente si descubre alguna llamada inusual o utilización de los datos en su factura.

9.- Compruebe regularmente si hay actualizaciones para el sistema operativo de su teléfono y aplicaciones importantes. Instálelas tan pronto como estén disponibles.

10.- Haga un uso inteligente del Wi-Fi y del Bluetooth. Cuando se conecta a Internet mediante Wi-Fi en un lugar desconocido, pruebe a utilizar una red encriptada que requiera contraseña. Si no es posible, evite la banca en línea o transacciones financieras en áreas públicas ocupadas y otra sin garantía de Wi-Fi de redes. Asegúrese de que los transeúntes no pueden ver lo que está escribiendo y desactive la opción Bluetooth cuando no lo esté utilizando.

11.- Copia de seguridad de sus datos regularmente. Configure su teléfono para que realice copias de seguridad de sus datos periódicamente o bien al sincronizar con su pc de sobremesa o portátil y para mayor seguridad de salvar los datos, realice una copia de seguridad de esos mismos datos en una tarjeta de memoria independiente.

12.- Si decide deshacerse de su teléfono y reciclarlo, asegúrese de borrar toda su información personal en primer lugar. La mayoría de los teléfonos tienen una opción para restablecer la configuración de fábrica. Recuerde quitar o limpiar cualquier tarjeta de memoria insertada.

13.- Para ayudarle en caso de robo de su móvil o pérdida, pida a su proveedor o al fabricante si tiene los servicios como el seguimiento de móviles y la capacidad de borrar de forma remota la información almacenada en el teléfono.

Si sigues estos consejos para la seguridad de tu movil o celular, conseguirás no llevarte ninguna sorpresa y disgusto con el tiempo.

consejos-seguridad-en-tu-movil

Profundizando en la Seguridad de Android

Fernando

Profundizando en la Seguridad de Móviles y Tabletas con Android

La Raiz de los Dispositivos

seguridad-de-moviles-tabletas

Por defecto, en Android el kernel y es un pequeño subconjunto de las aplicaciones centrales que se ejecutan con permisos de Root. ***Android no impide que un usuario o una aplicación con permisos de Root que pueda modificar el sistema operativo***, kernel y cualquier otra aplicación.

En general, al acceder a la raíz, ***se tiene acceso completo a todas las aplicaciones*** y todos los datos de la aplicación. Los usuarios que cambian los permisos en un dispositivo Android para permitir el acceso Root y a las aplicaciones, aumentan el riesgo para la seguridad de que aplicaciones maliciosas se instalen en el equipo y de lugar a defectos y errores de aplicación.

La capacidad tan grande de modificar un dispositivo Android, es importante para los desarrolladores que trabajan con la plataforma Android. En muchos dispositivos con este sistema operativo, los usuarios tienen la posibilidad de desbloquear el cargador de arranque con el fin de permitir la instalación de un sistema operativo alternativo. Estos sistemas operativos alternativos ***pueden permitir a un propietario obtener acceso Root*** y a los efectos de la depuración de aplicaciones y componentes del sistema o de las funciones de acceso no presentados a las aplicaciones de las API del software.

En algunos dispositivos, una persona con el control físico de un dispositivo y un cable USB es capaz de instalar un nuevo sistema operativo que proporcione privilegios de Root para el usuario.

Para proteger los datos de usuario existentes de compromiso el mecanismo de desbloqueo del gestor de arranque ***requiere que el gestor de arranque borre todos los datos de usuario existentes*** como parte de la etapa de desbloqueo.

El cifrado de datos con una clave almacenados en el dispositivo no protege los datos de la aplicación de los usuarios Root. ***Las aplicaciones pueden añadir una capa de protección de datos*** mediante el cifrado con una clave almacenada fuera del dispositivo, como en un servidor o una contraseña de usuario.

Este enfoque puede proporcionar protección temporal, mientras que la clave no está presente, pero en algún momento la clave debe ser proporcionada a la aplicación y entonces se convierte en ***accesible para los usuarios Root.***

seguridad-de-moviles-tabletas

Un enfoque más robusto para proteger los datos de los usuarios de la raíz es a través del uso de soluciones de hardware. Los fabricantes de equipos originales pueden decidir si la aplicación de soluciones de hardware que limitan el acceso a determinados tipos de contenidos tales como DRM para la reproducción de vídeo, o el almacenamiento de confianza relacionadas con NFC para Google.

En el caso de un dispositivo perdido o robado, el cifrado del sistema de archivos completo en los dispositivos Android utiliza la contraseña del dispositivo para proteger la clave de cifrado, por lo que modificando el gestor de arranque o el sistema operativo ***no es suficiente para acceder a los datos del usuario*** sin contraseña en el dispositivo del usuario.

Las mejores practicas de seguridad en Android

Fernando

CONSEJOS Y RECOMENDACIONES SOBRE LAS MEJORES PRACTICAS DE SEGURIDAD EN SISTEMAS CON ANDROID

El equipo de seguridad de Android recibe regularmente solicitudes de más información acerca de cómo ***prevenir posibles problemas de seguridad en los dispositivos*** que llevan instalado este sistema. Ocasionalmente, también realizará controles aleatorios de dispositivos y dejamos que los OEMs y socios afectados sepan de los problemas potenciales.

Seguridad-en-android

Este artículo ofrece a los OEM y otros socios, las mejores prácticas de seguridad en base a nuestras propias experiencias. Esto es un ampliación de la documentación para la Seguridad que hemos proporcionado para los desarrolladores, incluyendo las mejores prácticas que son únicos a los que están construyendo o instalando software a nivel de sistema en los dispositivos.

Siempre que sea posible, el equipo de seguridad de Android incorporará pruebas en el Android Compatibility Test Suite (CTS) y Android Lint para facilitar la adopción de estas mejores prácticas. Animamos a los socios a contribuir aportando pruebas que puedan ayudar a otros usuarios de de este sistema operativo.

Fuente revisión de seguridad de código

La fuente de revisión de código puede detectar una ***amplia gama de cuestiones de seguridad***, incluidas las indicadas en este artículo. Android alienta firmemente tanto la revisión de código fuente manual como la automatizada.

Las pruebas automatizadas

Las pruebas automatizadas pueden detectar una amplia gama de temas de seguridad, entre ellos muchos de los identificados en este artículo como los siguientes:

- *CTS se actualiza regularmente con pruebas de seguridad. La versión más reciente de CTS debe ser ejecutada para verificar la compatibilidad.*

- *CTS debe ser ejecutado con regularidad durante todo el proceso de desarrollo para **detectar problemas a tiempo** y reducir el tiempo de corrección. Android CTS utiliza como parte de la integración continua con nuestro proceso de construcción automatizado, que construye múltiples veces por día.*
- *OEM debe automatizar las pruebas de seguridad de las interfaces, incluyendo pruebas con entradas malformadas.*

Seguridad-en-android

La firma de las imágenes del sistema

La firma de la imagen del sistema es crítica para determinar la integridad del dispositivo y específicamente en:

- *Los dispositivos no deben estar firmados con una clave que se conozca públicamente.*
- *Las teclas utilizadas para firmar los dispositivos deben ser manejados de una manera consistente con las prácticas estándar de la industria para el manejo de las teclas sensibles, **incluyendo un módulo de seguridad de hardware (HSM)** que proporciona un acceso limitado y auditable.*

¡Cuidado! con los permisos de las Aplicaciones a instalar

Fernando

Instalar App: ¿Sí a todo los permisos que nos solicitan?

Examinando permisos de aplicaciones

En Android entre las pantallas que vemos en el momento de instalar una aplicación son los permisos que nos solicita que muchas personas no hacen ni caso limitándose a pulsar “siguiente”, seguir de forma directa a la siguiente pantalla para seguir diciéndole “aceptar y siguiente” hasta terminar de instalar el software aplicación en nuestro terminal móvil. Hay que admitir que la gran mayoría de personas emplean este sistema por “vaguería y comodidad”.

permisos-app-movil-2

Para quien le dé vagancia echar un ojo a esta clase de permisos de forma manual y descartar de esta forma posibles peligros, por ejemplo: ¿para qué nos solicita permiso a nuestra lista de contactos una aplicación de Linterna?, existen alternativas que automatizan el chequeo de nuestro móvil celular.

En definitiva; necesitamos “algo o alguien” que nos supervise los permisos a la hora de instalar cualquier aplicación en nuestro teléfono o tableta por muy “inocente” que esta parezca.

Muchos antivirus para Android ya integran esta funcionalidad. Hay aplicaciones dedicadas como por ejemplo: **Clueful Privacy Advisor** de BitDefender. Esta aplicación examina los permisos que nos solicitan las aplicaciones a instalar y nos informa cuales de ellas solicitan permisos sospechosos al revisarlos con una lista contrastada por la compañía de seguridad.

Bloqueo de llamadas: Spam telefónico

¿A que no es la primera vez que os llaman de otra operadora móvil o bien aun de la vuestra para “mejorar” la tarifa que tenéis? Bueno puesto que existe la posibilidad de bloquear esta clase de llamadas y hay muchas aplicaciones que dejan gozar de unas lista negra de teléfonos que bloquear, esto es, que si llaman de manera directa el móvil cuelga, sin siquiera sonar.

Lo más interesante en este punto no es comentaros qué aplicaciones hay, puesto que seguramente estemos frente al punto con más opciones. El modo perfecto de funcionamiento viene a ser redactar el número en esa lista o bien en determinados casos cuando recibimos una llamada, escogerlo e incorporarlo a dicha lista.

permisos-app-movil-1

No obstante queremos dejar perseverancia de ciertas aplicaciones que emplean bases de datos generadas por los usuarios que han identificado los números llamantes con los servicios que ofrecen pudiendo bloquearlos de forma directa. Ejemplo de ello es **Call Control** que ofrece un apartado Community en el que están clasificados estos servicios y podrás bloquearlos de forma directa.

Cifrado y más cifrado tras el escándalo de la NSA

La agencia estadounidense de inteligencia NSA, ha estado controlando y observando las comunicaciones de millones de personas en todo el mundo y este punto ha sido el detonante en el momento de empezar a usar cifrado en sus telecomunicaciones e intercambio de datos por muchos usuarios.

El Cifrado en nuestro móvil

En Android podemos cifrar el contenido del almacenaje interno de forma nativa desde el apartado de ***Seguridad*** en ***Configuración***. No obstante las comunicaciones que efectuamos y recibimos desde el terminal, bien sea correo electrónico, SMS, llamadas, navegación web, o bien desde cualquier aplicación dependen en gran medida del servicio que empleemos.

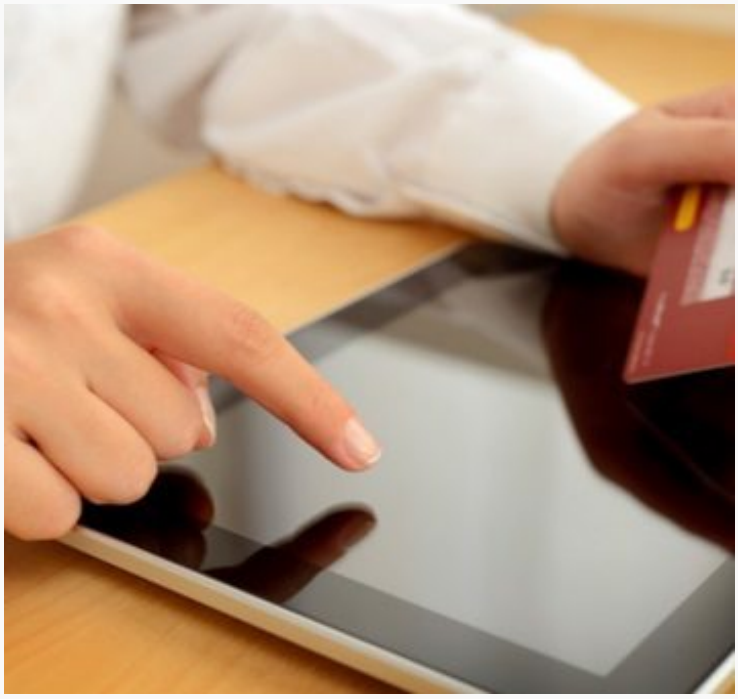
Hay ciertas opciones en el momento de efectuar llamadas “seguras” como por poner un ejemplo **RedPhone** que emplea cifrado VoIP para la comunicación. Es muy fácil de emplear y se integra con el empleo tradicional de las llamadas. Si advierte y detecta que los dos usuarios usan la aplicación les insta a pasar a modo seguro.

En este punto queremos recalcar y comentar, que existen soluciones de privacidad más completas como la que ofrece **Silent Circle** prometiendo un cifrado punto a punto entre terminales y dispositivos conectados.

Entre las más populares es **Cerberus**, que marcha como una aplicación residente que subsiste aun a flasheos y deja funcionalidades más avanzadas como por poner un ejemplo, enviar un mensaje al teléfono, hacer un reporte cuando se use y enviárnosla (Reporte del usuario “extraño”) entre otras muchas funcionalidades.

A pesar del esmero de Google (Android), nos hallamos con ciertas faltas en ese servicio puesto que si, por poner un ejemplo, queremos borrar remotamente el terminal, podemos hacerlo, mas eso no atañe al almacenaje externo: microSD. Y esta función sí que está cubierta por diferentes suites de seguridad, en vez de llamarlos antivirus propiamente dicho.

ESET Mobile Security deja, por poner un ejemplo crear una lista segura de contactos que recibirían el nuevo número de una tarjeta que se use en el terminal tal como el código IMSI y el código IMEI del dispositivo o efectuar la ubicación y borrado recóndito del terminal, tarjeta de memoria incluida.



permisos-app-movil-4

Aconsejamos echar un ojo al apartado Antivirus en tanto que no son pocos los que ofrecen funcionalidades afines y muchos de ellos, además son gratuitos.

Leer todo + entenderlo + aplicar el sentido común = La mejor Protección

Es verdad que muy frecuentemente los usuarios nos hallamos con inconvenientes de seguridad extraños a nosotros, inconvenientes en el diseño de una aplicación o bien un servicio web que podría causar o bien no algunos inconvenientes de seguridad y privacidad en nuestros terminales móviles. En estos casos estamos a la merced del desarrollador y una futura actualización que de fin a ese inconveniente.

No obstante es de sobra conocido y por costumbre, que en muchas ocasiones instalamos aplicaciones y ni leemos y ni préstamos atención a lo más mínimo, a los permisos que nos solicitan tal aplicación. Si vas por la calle y conoces a alguien que te parece interesante, es posible que llegues a conversar con él, o tomar un café, ect. Pero a priori, no se te ocurre darle una copia de tus llaves de casa, coche, etc o le dejar que cotillee tu agenda telefónica en tu móvil, o bien tus fotografías, conversaciones, etc.

Android seguridad

Puesto que lo mismo pasa con las aplicaciones. Un usuario ha de ser capaz de echar un ojo a los permisos que solicita una aplicación en el momento de ser instalada y distinguir si hay algo extraño o bien no lo hay y “parce” todo normal.

Obviamente una aplicación completa como **WhatsApp** solicita muchos permisos pues precisa acceder a la tarjeta de memoria o bien almacenaje para grabar datos, fotografías, vídeos y sonidos. Asimismo acceso a la red, leer la lista de contactos y considerablemente más datos.

No obstante, hay aplicaciones básicas que demandan una serie de requisitos que sería mejor eludir. Entre los últimos ejemplo fue **Brightest Lintern**, que prometía encender el led flash del móvil como linterna, pero lo que pretendía y realizaba es recopilar información de localización de los usuarios.

Y finalmente y no por esta razón menos esencial, siempre y en toda circunstancia debemos de tener cautela en el momento de navegar por redes inalámbricas abiertas y/o gratis, eludiendo introducir usuario y claves de acceso en páginas no cifradas, pues muchas de ellas son redes de engaño.

permisos-app-movil-3

Y como siempre decimos: ***"La mejor protección que existe, empieza por el SENTIDO COMÚN"***

Como evitar que te espien el telefono celular o tableta

Fernando

CONSEJOS Y RECOMENDACIONES PARA EVITAR QUE TE ESPÍEN EL TELÉFONO O TABLETA

Si te sientes incómodo cuando crees que te pueden estar espiando tu terminal móvil celular o tableta, tanto por algún Hacker como los Servicios de Inteligencia de cualquier país, practica estos consejos y recomendaciones y estarás más tranquilo cuando haces uso de tu aparato.

hacker-espiar-telefono

- **Pon el teléfono en modo avión durante la reproducción de juegos:**

La mayoría de los juegos no necesitan una conexión a Internet para funcionar, pero sus redes de anuncios si lo necesitan. Anular la conexión a la red, bloqueará los anuncios de visualización y detendrá la transmisión de tus datos personales, tanto por el juego, como por los anuncios de terceros. El modo avión también puede ayudar al juego de correr un poco más ligero y deprisa, pues el procesador deja de cargar los anuncios que solicita el juego.

- **Utiliza siempre que puedas, una red privada virtual (VPN) al conectarse a Internet:**

Una red privada vitual (VPN) encripta todo el tráfico de datos hacia y desde su teléfono, tableta o un ordenador mediante el enrutamiento a través del servidor de un proveedor de VPN. El uso de una VPN no evitará al 100% que las aplicaciones puedan transmitir sus datos personales, pero si hará que sea mucho más difícil para los espías o hackers a la hora de intentar interceptar esas transmisiones. Las aplicaciones VPN como Hotspot Shield o VPN Express se puede descargar desde la App Store de Apple y también desde la web oficial de Google Play Store.

- **Evita en la medida de lo posible las publicaciones en tus cuentas de redes sociales a través de las redes móviles, pues estas son mucho más vulnerables a los ataques de los espías:**

En su lugar de eso, espérate hasta que estés conectado, a la red de tu domicilio o lugar de trabajo, pues estas redes, si están bien configuradas, tienen contraseñas de seguridad Wi-Fi.

Y si aún quieres mayor seguridad, cuando lo hagas, es decir, cuando te quieras conectar a tus redes sociales, hazlo a través de una conexión segura HTTPS desde tu PC de sobremesa o portátil, pues son aún más difíciles de atacar por espías .

- **Instala el software HTTPS Everywhere:**

HTTPS Everywhere es un pluging para el navegador del PC de escritorio y está disponible para los navegadores Firefox, Chrome y Opera y los proporcionan gratuitamente a través de Electronic Frontier Foundation.

hacker-espiar-telefono

- **Apaga el sistema Wi-Fi, GPS y la geolocalización en tu terminal, mientras no los utilices:**

Estos sistemas de Wi-Fi, GPS y geolocalización, pueden servir y se pueden utilizar para identificar rápidamente tu ubicación. No los uses hasta que te sea estrictamente necesario. Es posible que tengas que ir a varios ajustes de cada aplicación para desconectar sobre todo la geolocalización. Si haces todo esto, a los espías y hackers se lo pondrás mucho más difícil por no decir casi imposible el que te puedan localizar, pues ya no podrán utilizar los datos de aplicaciones para decirles dónde estás o dónde has estado.

- **Apaga las conexiones de datos móviles celulares:**

Si no necesitas recibir actualizaciones constantes de tus aplicaciones, desconecta los datos de red móvil celular y conéctate a Internet sólo cuando lo hagas a través de una red segura protegida por contraseña Wi-Fi. Aún estando apagado este sistema, podrás seguir recibiendo mensajes de texto y llamadas de voz, y además alargarás la vida de la batería.

Si sigues estos simples pero seguros consejos y recomendaciones, evitarás la mayor parte de los ataques que te intenten hacer a tu móvil celular o tableta con intención de espiarte y hacerse con tus datos personales.

Y recuerda: "A veces el sentido común, es la mejor arma contra los Hacker y Espías que se encuentran en la red"

ALARMA: Agujeros de Seguridad en Moviles Celulares

Fernando

ALARMA: AGUJEROS DE SEGURIDAD EN MÓVILES CELULARES

La seguridad es importante en cada aplicación que tengamos en nuestros terminales de teléfono y celulares. Por supuesto que es así, pero si hay un grupo de aplicaciones móviles que los usuarios quieren estar seguros que son seguras, valga la redundancia, por encima de cualquier otra aplicación, es probable que sean las que están relacionadas con la banca móvil, donde se juegan el dinero. Y es por ello que debería prestar atención a la hora de operar con su terminal para no encontrarse **agujeros de seguridad en móviles** celulares.

agujeros-de-seguridad-en-moviles

Es sin duda una gran sorpresa, que un nuevo estudio ha encontrado que **el 90% de las aplicaciones de banca móvil de los principales bancos tienen vulnerabilidades de seguridad graves** que podrían poner en peligro los datos confidenciales del usuario.

¡Alarma!, ¡alarma!

Algunos investigadores de seguridad publicaron recientemente sus hallazgos después de investigar estas aplicaciones de teléfonos inteligentes y tabletas de una muy conocida marca y **encontraron vulnerabilidades en 40 de los 60 bancos más importantes** del mundo estudiados.

Y descubrieron que:

Menos del 20% de las aplicaciones de Banco móvil tienen un ejecutable habilitado independiente de posición (PIE) y Stack Smashing Protection. Esto podría ayudar a **reducir el riesgo de ataques** de corrupción de memoria.

El 40% de las aplicaciones auditadas **no validan la autenticidad de los certificados SSL** presentados. Esto los hace susceptibles a ataques del tipo MITM.

El 50% de las aplicaciones son vulnerables a las inyecciones de JavaScript a través de implementaciones UIWebView inseguras. En algunos casos, la funcionalidad nativa de iOS fue expuesto, lo que permite acciones

como el envío de SMS o mensajes de correo electrónico desde el dispositivo de la víctima.

El 90% de las aplicaciones, contenía varios enlaces no SSL en toda la aplicación. Esto puede **permitir a un atacante interceptar el tráfico e inyectar código JavaScript** arbitrario HTML en un intento de crear una petición de inicio de sesión falsa o una estafa o engaño similar.

El estudio increíblemente preocupante saca a la luz un problema muy grave para el sector bancario y por ente, para los consumidores y usuarios de estas aplicaciones que tienen instaladas en sus teléfonos móviles celulares y/o tabletas.

agujeros-de-seguridad-en-moviles

Estamos convencidos que con el tiempo, habrá medidas más estrictas y seguras para este tipo de aplicaciones tan sensibles como la banca móvil, pues este uso de aplicaciones está creciendo mucho con el paso de los años.

El informe señala que las diversas vulnerabilidades de seguridad que se han descubierto e identificado, podrían **permitir a los hackers maliciosos interceptar datos confidenciales**, instalar software malicioso o incluso tomar el control del dispositivo de la víctima.

Las aplicaciones bancarias de toda la vida que han sido adaptados para dispositivos móviles, como teléfonos inteligentes y tabletas, han creado un problema de seguridad importante para las firmas financieras de todo el mundo y como conclusión se podría decir que a medida que esta **investigación a puesto al descubierto estos peligros de seguridad**, las entidades financieras deben aumentar los estándares de seguridad que utilizan para sus soluciones de banca de a través de estos dispositivos móviles.

Un consejo: *consulte en su banco, que medidas de seguridad tiene su aplicación de banca electrónica en su móvil celular. Y ante cual duda, no la use, evitará disgustos.*

agujeros-de-seguridad-en-moviles