Aplicaciones de móvil, un filón para el espionaje

TENDENCIAS 22 Y 23

Juegos de espías

Las aplicaciones de móvil, otro agujero por el que podemos llegar a perder nuestra privacidad

FRANCESC BRACERO
Barcelona

De estupor, en estupor, las revelaciones de Edward Snowden nos han descubierto un mundo en el que nuestros teléfonos se han convertido en herramientas capaces de revelar cualquier aspecto de nuestra vida a agencias gubernamentales, en especial a la Agencia de Securidad Nacional (NSA) de Estados Unidos. Este organismo de espionaje no sólo posee un imaginativo, amplio y prodigioso arsenal de soluciones técnicas para espiar cualquier teléfono, sino que también puede acceder a datos particulares a partir de las aplicaciones que nosotros mismos descargamos en nuestros móviles, según las últimas filtraciones. Hasta existe un método por el que se llegaron a espiar teléfonos con el popular juego Angry Birds, aunque la compañía propietaria de la *app*, Rovio, ha declinado cualquier responsabilidad en ello.

Josep Prieto, director del programa de informática de sistemas de la Universitat Oberta de Catalunya (UOC) y miembro del grupo de investigación Kison (acrónimo en inglés de criptografía y seguridad de la información para redes abiertas), advierte: "Cuanta más información tienes sobre seguridad, más inseguro te sientes. No por tener más información podrás estar más protegido". "Además, la seguridad perfecta no existe", recuerda.

Los expertos señalan que la vulneración de la privacidad a partir de aplicaciones de móvil se lleva a cabo por dos sistemas. Por una parte, cualquier aplicación es capaz de acceder a diferentes recursos del teléfono siempre que le autoricemos a ello. Por eso, es importante que, cuando utilicemos una *app* por primera vez, tengamos claro qué permisos le damos. Por ejemplo, si la aplicación es de un juego y nos pide el acceso a nuestra lista de contactos, lo más prudente es rechazar la petición. En caso contrario, indica Prieto, podemos estar dando accesos a "muchísima información, incluidas claves bancarias", sin darnos cuenta.

Otro gran peligro es que la aplicación haga uso de nuestros datos sin advertirnos porque los desarrolladores de la *app* han actuado de forma maliciosa. David

¿PÁJAROS ESPÍA?

Las últimas filtraciones revelan que la NSA usó el juego Angry Birds para obtener datos

¡OS FRENTE A ANDROID

Los especialistas creen que la tienda de Apple es más segura que la de Google

LAS PRINCIPALES TENDENCIAS DEL MERCADO DE 'APPS'

España, Top 10
La tienda de *apps* **Google Play** sitúa a **España** como **novena** en descargas en el 2013

Caramelos contra pájaros
Candy Crush se impuso como juego **número 1** mundial en el 2013 y **Angry Birds** fue **sexto**

Crece el 'freemium'
El modelo de **juego gratis**, pero con pagos dentro de la *app* (**'freemium'**) fue del **93%** en el 2013, frente al **86%** del año 2012

Facebook es móvil
Aparte de los **juegos**, lo más descargado del 2013 fue la app de **Facebook**

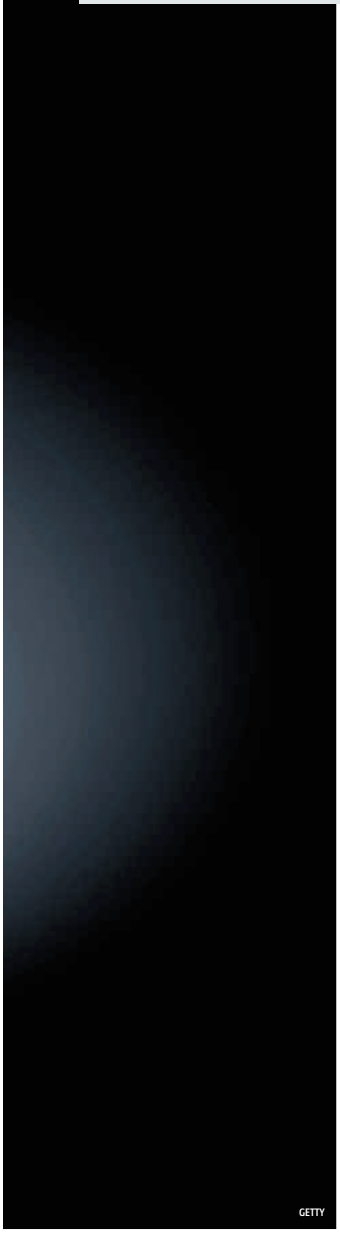
La utopía del internet sin riesgos

Telegram Un fenómeno por ser ¿seguro?

Uno de los grandes fenómenos en el campo de las aplicaciones en las últimas semanas es la aplicación Telegram, que está teniendo un crecimiento vertiginoso en numerosos países, incluido España, donde aseguran que han llegado a un ritmo de 200.000 nuevos usuarios diarios. Se trata de una *app* de mensajería al estilo de WhatsApp, pero sus creadores, los propietarios de la red social rusa VKontakte, ofrecen una recompensa de 200.000 dólares a quien rompa su protocolo de encriptación de mensajes. En estos momentos hay expertos que examinan la documentación abierta que ofrece Telegram y que intentan poner a prueba su seguridad. En cualquier caso, seguridad en la encriptación de los mensajes, de forma que sólo el emisor y el receptor final sean capaces de leerlos, no significa respeto a la privacidad. De hecho, en la lista de contactos de Telegram podemos ver quiénes, entre nuestra lista de contactos, se encuentran conectados y cuándo fue la última vez que accedieron al programa. Tanto WhatsApp, desde hace más de un año, como otras aplicaciones de mensajería (por ejemplo Spotbros) utilizan sistemas de encriptación para evitar que los mensajes puedan ser interceptados por terceros ajenos a una comunicación.

Blackphone En busca del móvil antiespías

Durante el próximo Mobile World Congress, que se celebrará en Barcelona del 24 al 27 de febrero, se presentará un modelo de teléfono, el Blackphone, que pretende ser seguro ante las amenazas a la privacidad. Este móvil, creado por la firma española Geeksphone y la norteamericana Silent Circle, experta en encriptación de datos, funciona con una versión especial del sistema operativo Android llamada PrivateOS. El comunicado de la compañía sobre este modelo indica que "proporciona tanto a individuos como a organizaciones la posibilidad de realizar y recibir llamadas seguras, intercambiar mensajes de texto seguros, transferir y almacenar ficheros, y videoconferencias sin comprometer la privacidad del usuario al utilizar el terminal". El consejero delegado de Geeksphone asegura que el Blackphone "es una oportunidad excelente no sólo para innovar en tecnología sino para permitir a los usuarios que se comuniquen de forma segura, cosa que ahora mismo es imposible". El consejero de Silent Circle, Phil Zimmerman afirma que el móvil ofrecerá a los usuarios "todo lo que necesitan para asegurar la privacidad y el control de sus comunicaciones, a la vez que otras características superiores que se esperan de un *smartphone*".


GETTY

Megías, doctor ingeniero en informática y profesor de la UOC, explica que cuando se instala una aplicación aparecen textos en la pantalla que nadie lee. Si lo hiciéramos, "muy a menudo no instalaríamos determinadas aplicaciones, a las que damos sin saberlo acceso al registro de llamadas, a los contactos y a los correos".

Este último comportamiento del usuario podría ser el que hay detrás de la brecha de seguridad que ha implicado a Angry Birds. Se trata de la versión gratuita del juego para Android. que contenía publicidad. Según Rovio, ha sido una de las firmas que se encargaba de la publicidad la que habría hecho un uso fraudulento de los datos de los usuarios del juego para hacerlos llegar a la NSA.

CONSCIENCIA

Los expertos alertan de que es muy difícil tener privacidad completa con las 'apps'

IMPRUDENCIA

Muchos usuarios aceptan los permisos que la 'app' pide al usarla por primera vez

El investigador de la UOC Alexandre Dotor cree que hay que mantener dudas tanto sobre las acusaciones a Angry Birds como sobre la certeza de que Rovio no sabía nada. Este experto cree que la empresa podía saber que la NSA "accedía a los datos", pero señala que si la filtración era a través de la publicidad "podrían estar afectadas muchísimas más aplicaciones que Angry Birds".

El permiso de las aplicaciones para acceder a nuestros datos puede venir asociado a una determinada funcionalidad básica de la *app*, para facilitar que le demos nuestra aceptación y a veces se presenta de forma pequeña o con colores que se confunden con el fondo de la pantalla.

La UOC elabora decálogos de seguridad

Varios expertos de la Universitat Oberta de Catalunya (UOC) han elaborado cuatro decálogos sobre seguridad en relación con la vida digital. Se trata de ofrecer a la sociedad información clara y sencilla sobre cómo actuar en relación con el acceso a internet, el comercio electrónico, las contraseñas y la aplicación de mensajería WhatsApp.

Los expertos, coordinados por Josep Prieto, director de los estudios de Informática, Multimedia y Telecomunicaciones, son la profesora Helena Rifà-Pous, y los investigadores Alexandre Dotor Casals, Joan Arnedo y Josep Jorba.

Prieto explica que, como miembros de la comunidad universitaria y como grupo de seguridad informática de referencia (Kison), se pusieron como objetivo "poder llegar a la sociedad y que la universidad aporte valor". Los decálogos pretenden "dar instrucciones lo más claras posibles" sobre los comportamientos seguros en relación con internet.

La regla más básica que siempre se recomienda a los usuarios en general es que tengan en cuenta que los dispositivos móviles y el ordenador siempre están conectados a internet. "Todo el mundo te escucha", resume Prieto. Así que, "cuando instalas algo, tienes que pensar que cualquiera te puede estar observando. Esto te hará más consciente de lo que puedes hacer".

Muchos de los aspectos que recogen en los decálogos son de sentido común.

Por ejemplo, hay que asumir que lo que se pone en una red social no estará circunscrito a un círculo reducido de personas y que podrá llegar a otros ámbitos. De la misma forma, hay que calcular que lo que hoy nos hace gracia ver en internet quizás nos moleste dentro de unos años, o comprometa nuestra vida profesional.


ANDREW KELLY / REUTERS

El móvil, siempre conectado

Otro elemento delicado son las contraseñas, en las que hay que evitar palabras que estén en el diccionario, porque un ordenador puede descifrarlas, así como datos personales como fechas de nacimientos o secuencias de números del tipo 1,2,3,5,6.

De la misma forma, es peligroso utilizar wi-fi público para acceder a la cuenta bancaria, porque puede ser accesible para otros, o no proteger adecuadamente la red wi-fi doméstica. En este caso, se recomienda el protocolo WPA2.

"Ni los expertos en informática podemos estar seguros de que las aplicaciones que instalamos son seguras –apunta Prieto–. así que para un usuario normal es muy difícil". Una recomendación básica es recurrir a las tiendas oficiales de *apps*, donde es más difícil que haya aplicaciones maliciosas. Los expertos aseguran que Apple "es bastante más cuidadosa que Google" con las aplicaciones que tiene disponibles. "Hacen un mayor control de las *apps*", afirma Megías.

Josep Prieto sugiere que una buena solución sería la creación de algún portal independiente que mantuviera información actualizada sobre la seguridad de todas las *apps* del mercado. Megías cree que tampoco es bueno "transmitir la idea de que estamos totalmente desprotegidos" y vislumbra la esperanza de una mejor privacidad en el hecho de que "hay gente que por afición se dedican a analizar el código de las *apps* para ver qué hacen". Así se han descubierto algunas violaciones de la privacidad.

En muy pocos años hemos pasado de teléfonos que hacían poco más que llamar, a sincronizar correos, proyectos profesionales, documentos personales y otros datos sensibles. Alexandre Dotor considera que hay "una inconsciencia general muy grande con los smartphones, en los que los datos son muy críticos".

En los teléfonos llevamos información susceptible de complicarnos la vida en caso de que caiga en manos ajenas, así que, aunque la seguridad no sea perfecta, hay que ser prudentes ante todo.●

APRENDA MÁS SOBRE LAS 'APPS' EN EL CANAL DE TECNOLOGÍA DE **www.lavanguardia.com/tecnologia**