APPS ›

Cómo saber cuándo una 'app' accede a la ubicación, la cámara o el micrófono del móvil

Los expertos en ciberseguridad insisten en instalar solo las aplicaciones estrictamente necesarias

ISABEL RUBIO

6 AGO 2019 - 17:57 CEST

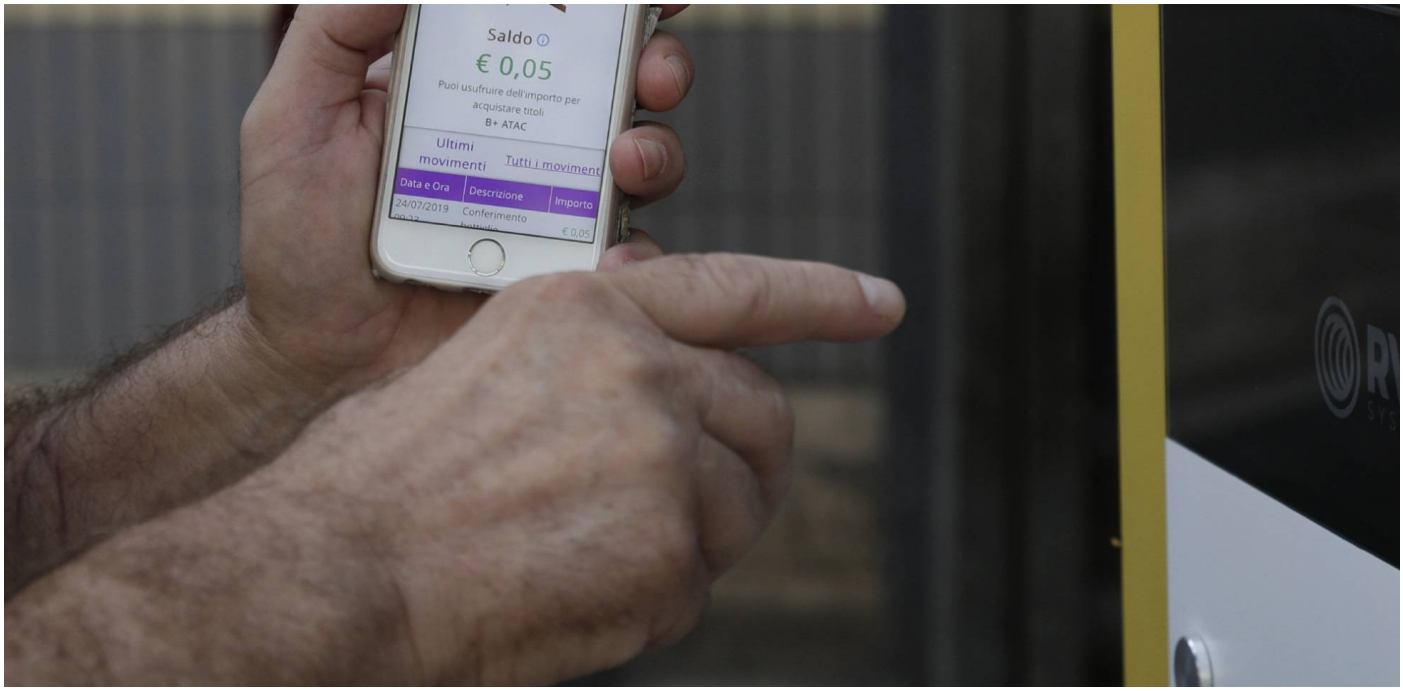
Un usuario sostiene un 'smartphone' con múltiples aplicaciones. PIXABAY

"Oye @Aeromexico ¿por qué están tratando de usar la cámara de mi celular?". Con este tuit, el periodista británico Duncan Tucker preguntaba hace unas semanas a la aerolínea porque había intentado acceder a la cámara del teléfono cuando, además, tenía el permiso pertinente desactivado. Prácticamente todas las aplicaciones en el mercado recopilan datos de los usuarios y tienen acceso a determinados permisos. Pero en muchas ocasiones al usuario se le escapa en qué momento las aplicaciones los utilizan y si lo hacen de forma lícita. ¿Es posible saber cuándo una aplicación accede a la cámara, las fotografías o el micrófono de un teléfono móvil?

Javier Tallón, miembro del Grupo de Seguridad Informática y para la Defensa del Consejo de Colegios de Ingeniería Informática, explica en referencia al caso de Tucker que el acceso a la cámara por parte de la aerolínea mexicana podría ser lícito en algunas situaciones. Por ejemplo, en el caso de que se estuviese usando para la lectura de códigos de los billetes. Pero, a juzgar por el tuit del periodista, la aplicación intentó acceder a este permiso en un momento en el que no correspondía.

Tucker descubrió las intenciones de la aerolínea mexicana porque tenía activado en su *smartphone* el "monitor de permisos de aplicaciones". Se trata de una función solo disponible para algunos terminales de Samsung que permite dar permisos a la carta a cada aplicación y saber cuándo hace uso de ellos. "Recibe notificaciones cuando las aplicaciones que se estén ejecutando en segundo plano utilicen los permisos que has seleccionado", se informa al ir a activar la función en los ajustes del teléfono. Además, toda esta actividad queda registrada en un historial que el usuario puede revisar en cualquier momento.

El monitor de permisos en este caso alerta de la intención y no tanto de la ejecución, según subraya Tallón, que también es cofundador y director técnico y de operaciones de jtsec Beyond IT Security: "Podemos pensar que, al tratar la aplicación de usar la cámara, el monitor de permisos detecta que hay un comportamiento sospechoso y lanza la alerta. Sin embargo, la aplicación nunca pudo llegar a acceder a la cámara del dispositivo al estar el permiso desactivado".



Un usuario utiliza una aplicación móvil. **GREGORIO BORGIA (AP)**

A qué información accede cada aplicación

Normalmente, un usuario puede conocer el listado de permisos que necesita una *app* para funcionar en el momento de su instalación. Las *apps* suelen solicitar al usuario una media de entre tres y cuatro permisos, según afirma Tallón. Los permisos más solicitados, según sostiene, son el acceso a archivos del usuario, a la cámara del dispositivo y a los servicios de localización. Y las aplicaciones que tienden a solicitar la mayor cantidad de permisos son las relacionadas con redes sociales y compras *online.*

"Una vez instalada la aplicación, podemos conocer la primera vez que hace uso de cada permiso, ya que solicitará su ejecución al usuario", explica Ismael Morales, miembro del Grupo de Seguridad Informática y para la Defensa del CCII y technical cybersecurity manager en Wellness TechGroup. Después, las aplicaciones no necesitarán consentimiento del usuario cada vez que usen los permisos anteriormente aceptados: "A partir de este punto, el usuario ya no sabe cuándo las aplicaciones hacen uso de los permisos".

De hecho, la función del móvil de Tucker solo está disponible en algunos móviles de Samsung y no es común en el resto de terminales. "Es difícil para un usuario corriente saber a qué información tiene acceso una aplicación o el propio dispositivo más allá del control de permisos", asegura Tallón. Para protegerse, los expertos consultados recomiendan instalar solo las *apps* que realmente se necesiten y fijarse antes de hacerlo

en si los permisos solicitados pueden ser abusivos. Morales aconseja que en el caso de contar con varias alternativas al instalar una aplicación que ofrece la misma funcionalidad, es preferible instalar la que menos permisos que consideremos abusivos solicite.

Tres hombres hablan por teléfono móvil. **EFE**

Herramientas

El investigador del ICSI Serge Egelman explica que existen muchos sitios web y herramientas que muestran qué permisos son solicitados por una aplicación, pero no informan de si esos permisos se usan realmente en la práctica ni del momento preciso en el que se utilizan: "Saber que se solicita un permiso no es lo mismo que saber que realmente se usó".

Para detectar qué permisos usa una aplicación y en qué momento lo hace, según señala, debe de modificarse el sistema operativo. Él lo ha hecho con un grupo de investigadores y ha creado AppCensus, una compañía que se encarga de verificar el comportamiento de diferentes *apps* de Android. "Durante varios años, hemos estado construyendo nuestra propia versión personalizada de Android que incluye instrumentación para monitorear el acceso de las aplicaciones a los datos personales. Debido a que esto requiere modificaciones del sistema operativo, no se puede hacer en una aplicación que se instala desde Play Store", afirma.

AppCensus facilita en su web información sobre los comportamientos de diferentes *apps* en el mercado para que el usuario pueda saber a qué datos acceden y si son compartidos con terceros. Se trata, según Egelman, de una de las pocas formas de que los consumidores entiendan las implicaciones de privacidad de las aplicaciones que usan". Subraya que antes solo había dos formas de saberlo: leer las políticas de privacidad y examinar el tráfico de la red. "Todos conocemos los problemas con las políticas de privacidad. Son ambiguas, requieren mucho tiempo y son difíciles de leer. En segundo lugar, esperar que el usuario promedio monitoree y analice el tráfico de la red es simplemente absurdo, además de que significa que para cuando detecta un mal comportamiento, este ya ha pasado", añade.

Joel Reardon, profesor asociado de la Universidad de Calgary y otro de los artífices de AppCensus, cuestiona la usabilidad de una herramienta que constantemente le informe al usuario de que una *app* va a utilizar su permiso. Para él, sería útil que el usuario pudiera, por ejemplo, negar el acceso a la ubicación, el micrófono o la cámara cuando la pantalla o el audio del terminal estuvieran apagados.

Tanto Egelman como Reardon hacen hincapié en que algunas aplicaciones buscan la forma de acceder a determinada información aunque el usuario les haya denegado el permiso de forma explícita. Ambos han participado en una investigación llevada a cabo por un equipo de expertos en ciberseguridad, que ha revelado que hasta 12.923 *apps* han encontrado la forma de seguir recopilando información privada pese a haberles negado los permisos explícitamente. El número de usuarios potenciales afectados por estos hallazgos, según señalan, es de "cientos de millones".

CONSEJOS PARA PROTEGERSE COMO USUARIO

Desarrolladores de aplicaciones e incluso fabricantes de terminales recopilan frecuentemente información de los usuarios sin su consentimiento. Así lo afirma Tallón, que señala que existe una diferencia considerable en la calidad de los smartphones de diferentes fabricantes: "Aunque, la tendencia es a pensar que los fabricantes más conocidos son los más confiables, resulta evidente que el tráfico de información de usuarios a gran escala es un negocio muy lucrativo y en el que participan, muy probablemente, la mayoría de las grandes empresas del mundo de los smartphones".

Por ello, señala que lo ideal es tratar de usar dispositivos cuya seguridad haya sido verificada y certificada por profesionales del sector independientes de los fabricantes. "Por ejemplo, en España tenemos la certificación LINCE, que ha sido publicado recientemente

por el Centro Criptológico Nacional y que está orientada a garantizar un nivel básico de seguridad y a comprobar este tipo de comportamientos en diferentes productos".

Por su parte, Morales advierte de que "uno de los puntos más débiles de un *smartphone* es la carga del mismo". Según explica, existen cables para cargar el móvil que no permiten el intercambio de datos cuando, por ejemplo, se conecta el móvil a un ordenador. "En este caso, una de las medidas principales es intentar evitar la carga de móvil con un cable que no sea exclusivamente de carga en lugares públicos", afirma.

ARCHIVADO EN:

Apps · Aplicaciones informáticas · Telefonía móvil multimedia · Telefonía móvil · Seguridad internet · Software · Empresas · Internet · Tecnologías movilidad · Telefonía · Informática · Telecomunicaciones

La comentada frase de Jaime Peñafiel sobre Juan Carlos I: no ha...

HUFFINGTON POST

En el corredor de la muerte, la serie sobre Pablo Ibar

EL PAÍS

Britney Spears recibe un nuevo golpe por la custodia de sus hijos

TIKITAKAS