Adriana Lizeth Dominguez Espinosa. 1811392

Es útil saber cuál es la forma con la que puedes revolcarle el acceso a estas aplicaciones para que dejen de obtener tus datos. El proceso es sencillo, pero no puedes hacerlo a través de las aplicaciones móviles, y tendrás que recurrir a la página web oficial.

Alrededor del 83% de las aplicaciones que instalamos en nuestros móviles les permitimos acceder a datos sensibles como contactos, llamadas o mensajes e incluso a manejar controles importantes de administración del dispositivo, como el apagado y encendido, el acceso a los datos del wifi o el accesos a los archivos de firmware.

Encontramos una aplicación que nos interesa y la descargamos en el móvil, pero nuestro dispositivo Android detecta que la app solicita permisos de uso considerados peligrosos y solicita la aprobación por nuestra parte.

A pesar de la fama de poco seguro que ha acumulado desde siempre el mercado de aplicaciones Android, existe un sistema de vigilancia muy eficaz entorno a los permisos de aplicaciones y que al funcionar en aislamiento de procesos garantiza que para determinadas acciones se precise la autorización precisa del sistema operativo.

Estos son los datos más sensibles de tu teléfono
Acceso al calendario. Permite tanto leer como editar y crear nuevos eventos en el calendario. El peligro está en que modifique algo importante o se elimine del calendario. Además puede usarse para controlar a un usuario al conocer la actividad que está realizando en cada momento.

Acceso a los contactos. Con este permiso la aplicación solicita poder entrar en nuestra lista de contactos, editarla, añadir nuevos y también acceder a la lista de cuentas de servicios cuyo acceso tengamos activado a través del móvil. Evidentemente esto puede suponer un filón para los que se ganan la vida enviando *spam* o incluso para los estafadores, más aún en el caso de entrar sin permiso en nuestras cuentas y actuar de manera fraudulenta con nuestros perfiles.

Adriana Lizeth Dominguez Espinosa. 1811392

Acceso a las cámaras. Permitimos a una app tomar fotos y grabar vídeos por sí misma con el asalto a la intimidad que puede suponer esto, sobre todo si cae en malas manos.

Acceso al almacenamiento o memoria. Ya sea a un sistema de almacenamiento externo como la tarjeta SD o al almacenamiento interno, donde se autoriza a que lo lea o incluso a que almacene allí archivos. El peligro está, obviamente en la recopilación de nuestros datos, pero también en la copia o destrucción de archivos de interés que podamos custodiar.

Acceso al micrófono. Al permitir el acceso de la app a nuestro micrófono nos exponemos a que se graben nuestras conversaciones telefónicas o incluso actuar de micrófonos espía en cualquier otro momento.

Acceso a mensajes de texto. Permite que la aplicación envíe mensajes de texto (SMS, MMS o incluso mensajes tipo push WAP) lea los mensajes guardados o reciba nuevos. Hay que tener especial cuidado con este permiso, ya que es el que más utilizan los ciberdelincuentes para suscribirnos a servicios de pago no deseados.

Acceso a sensores corporales. Permiso ligado con el uso de *wearables*. Con ello damos datos sobre nuestra salud que normalmente pertenecer a nuestra vida privada.

Acceso a la ubicación. Permitimos que la app sepa en todo momento donde nos encontramos, bien a través de GPS, bien a través de las antenas móviles o el wifi. Esto puede ser usado por delincuentes para saber en qué momento no estamos en casa y también puede suponer una intrusión agresiva de publicidad a través de notificaciones, por ejemplo, las que nos piden que valoremos el restaurante en el que acabamos de comer o que subamos a una red social la foto que acabamos de hacer en un determinado lugar.

Adriana Lizeth Dominguez Espinosa. 1811392

Acceso al teléfono. Con ello autorizamos a leer el estado del teléfono, saber el número del mismo, conocer el estado de la red móvil, hacer llamadas, conocer el histórico de las mismas, añadir mensajes de voz, gestionar llamadas colgando o descolgando e incluso redireccionando a otro número. El peligro está en que la app conocerá todos los datos de voz que se hayan hecho desde el móvil y además puede hacer llamadas a servicios de pago sin nuestro consentimiento.

Además están los **permisos adicionales** o permisos de acceso especial. Suelen ser permisos específicos de algunas apps. Hay que vigilarlos especialmente por ser la puerta de entrada habitual de los virus y *malware*.