Seguridad en las apps

Antes de instalar una aplicación, analice si los permisos que solicita son los que realmente requiere para funcionar. Y ante la duda, no la instale.

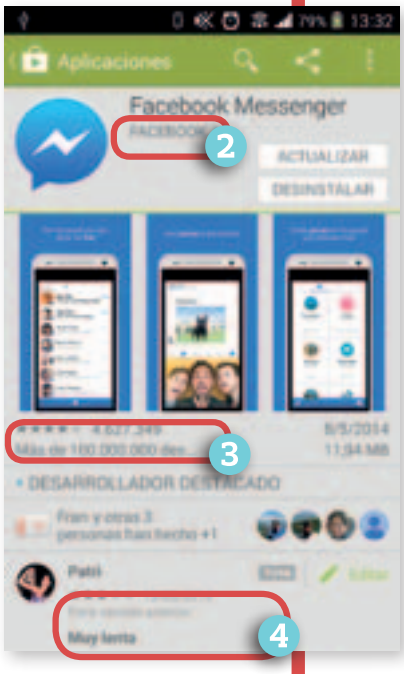
1 Antes de descargar, compruebe

Estas cuatro medidas pueden ser suficientes para proteger su información personal y evitarle más de un susto.

1 BUSQUE FUENTES FIABLES
A la hora de descargarse una app de internet, elija un sitio que sea conocido (Play Store, Amazon, Apple Store...). Evitará virus innecesarios. Por ejemplo, los "blackmarket" pueden darle más de un susto.

2 ELIJA UN DESARROLLADOR OFICIAL
Para una misma app habrá muchas sugerencias, lo más seguro es que instale la del desarrollador oficial.

3 FÍJESE EN EL Nº DE DESCARGAS
Si la app se la han descargado menos de 1.000 personas es probable que, si da algún problema, todavía no haya sido detectado.



4 LEA LOS COMENTARIOS
Si la aplicación tiene algo raro, casi seguro que alguién lo habrá escrito en los comentarios.

2 No acepte los permisos sin leerlos

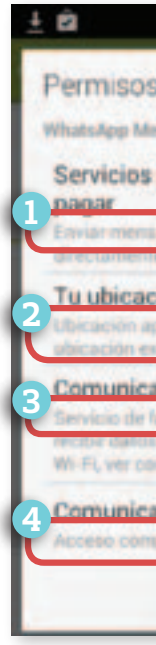
Cuando vaya a instalar una aplicación lea los permisos . Si le parece que algunos son sospechosos, lo mejor es que no la instale y busque otra aplicación que haga los mismo. Le mostramos algunos ejemplos.

1 MENSAJES
Si quiere instalar una aplicación para enviar mensajes, como WhatsApp, es normal que le pidan ciertos permisos. Ahora bien, si se trata de instalar un juego o de la aplicación de linterna, por ejemplo, entonces, ¡ojo!, lo más probable que se trate de un SMS Premium.

2 UBICACIÓN
Piense si la aplicación que se va a descargar realmente necesita este permiso, es decir, necesita saber todo el rato donde se encuentra usted o si, por el contrario, se trata de un abuso de su privacidad.

3 SERVICIO DE FACTURACIÓN GOOGLE PLAY
Si la app es gratuita pero requiere este permiso, seguramente se trate de una compra integrada o de pago; es decir, compras adicionales que pueden realizarse dentro de una app ya descargada. Muchos juegos gratuitos utilizan este sistema (Candy Crash), donde para avanzar niveles le ofrece la posibilidad de pagar.

4 ACCESO COMPLETO A LA RED
Si le piden este permiso, por ejemplo, para la aplicación de linterna, donde solo deberían pedirle acceso a la cámara para activar el flash, lo más probable es que se trate de anuncios de publicidad. El riesgo de este permiso es que su uso combinado con otros, por ejemplo, el de acceso a sus contactos, vulnera su privacidad.



Nuestros contactos, los sitios donde vamos, cómo empleamos nuestro tiempo libre, qué leemos... en definitiva, nuestra vida personal se encuentra almacenada en nuestro smartphone. Y en un mercado como el de hoy en día, en el que el marketing personalizado lo es todo, estos datos tienen mucho valor. De ahí, que muchos desarrolladores de aplicaciones, para conseguirlos, se extralimiten con los permisos que reclaman de nuestros móviles llegando a vulnerar nuestra privacidad. En este artículo le ayudamos a tomar ciertas precauciones para que esto no le ocurra.

Se debe respetar más nuestra privacidad

Garantizar la privacidad de los usuarios debería ser una prioridad. Sin embargo, no todos los sistemas operativos cuidan este tema permitiendo que algunos desarrolladores la vulneren. Por ello, pedimos que, independientemente del sistema operativo de nuestro teléfono, el usuario pueda ver, antes de proceder a la descarga de la aplicación, qué permisos requiere y con qué fin van a usarse. Además, los usuarios deben poder rechazar uno por uno aquellos permisos que creen que vulneran su privacidad, sin que por ello tengan que renunciar a la aplicación por completo, como ya hace Apple en su sistema operativo.

3 Y configure su móvil

Según el sistema operativo que tenga, le resultará más sencillo gestionar la privacidad y seguridad de su móvil. Como verá en los ejemplos, a la cabeza se encuentra Apple.

COMPRA DE APLICACIONES

1 **APPLE iOS7** Apple Store indica explícitamente debajo de cada aplicación que usted puede hacer compras dentro de esa app (compras integradas) y cuál es su coste. Pero, también le permite desactivar esta opción.
Apple cuenta, por defecto, con una contraseña de compra que dura 15 minutos. Aunque, para mayor seguridad le da la posibilidad de solicitar "una contraseña de inmediato", para que la introduzca siempre que se haga una compra (vea ilustración).

ANDROID 4.3 Google no soluciona el problema de las compras integradas: no cuenta con un tiempo para echarse atrás y las reclamaciones deberá hacerlas al desarrollador de la aplicación. Tampoco, tiene una contraseña por defecto. Si usted quiere poner una para evitar gastos inesperados, tendrá que hacerlo en Play Store› Ajustes›Contraseña.
No obstante, una vez que la ha introducido, durante 30 minutos no se la volverán a solicitar, de manera que en ese tiempo sus hijos podrían descargarse lo que quisieran.

GESTIÓN DE PERMISOS

2 **APPLE iOS7** Le permite ir aplicación por aplicación aceptando los permisos que crea oportunos. A medida que las aplicaciones instaladas le vayan pidiendo nuevos permisos, le irán apareciendo en este apartado.
También podrá gestionar los servicios de localización y desactivarlos (vea ilustración).
Su store está muy controlado evitando que los desarrolladores se extralimiten en exceso con los datos que toman de los móviles.
No obstante, recuerde que si desactiva algún permiso básico de alguna aplicación, podría dejar de funcionar correctamente.

ANDROID 4.3 Si usted rechaza uno de los permisos que requiere la app, simplemente no le dejará descargársela.
Además, en Android los desarrolladores tienen más libertad para recopilar todo tipo de datos. Usted solo podrá consultar los que están usando las apps que se ha descargado entrando en Ajustes›aplicaciones›descargas.

WINDOWS PHONE Este sistema operativo ni siquiera le muestra los permisos que utiliza cada app. El desarrollador tiene libertad para mostrarlos o no.