ILUSTRACIÓN **ADOBE STOCK**

El test para descubrir que la app que quieres es segura. Hay casi una para cada cosa que hacemos, pero no todas son fiables

J. C. CASTILLO

Las aplicaciones que usamos a diario han convertido nuestros ordenadores, tablets y smartphones en improvisadas navajas suizas. Existe una prácticamente para cada cosa: realizar mediciones con la cámara del teléfono, encontrar la gasolinera más barata, consultar la presencia de medusas en una playa concreta... Millones de desarrolladores alrededor del mundo se rompen la cabeza para encontrar usos prácticos que poder transformar en la app de moda.

Las cifras hablan por sí mismas: solo en 2024 se descargaron más de 137.000 millones de apps a nivel global y, a falta de estadística oficial, en 2025 habrán sido más de 299.000 millones. Esto supone la descarga de 258.000 apps por minuto... y el empleo de 26 al mes por parte de un usuario promedio. Queda claro que sabemos cómo descargarlas, pero ¿seguro que lo estamos haciendo con seguridad?

La Oficina de Seguridad del Internauta (OSI), que depende del Instituto Nacional de Ciberseguridad (Incibe), ofrece algunas pautas para confirmar de que aquello que instalamos y usamos en nuestros dispositivos no entrañe riesgo alguno. La primera regla es fácil: consiste en descargar aplicaciones a través de las tiendas oficiales de las diferentes marcas. Por ejemplo, en Windows intentaremos recurrir siempre a la 'Microsoft Store', mientras que en un sistema macOS optaremos por la 'App Store' de Apple.

Si hablamos de teléfonos móviles, resultan ampliamente conocidos la 'Play Store' de Google (con más de 113.000 millones de descargas anuales) y la 'App Store' de Apple (35.000 millones), aunque conviene matizar que su seguridad no resulta inquebrantable. Se han dado múltiples casos de apps maliciosas que han sorteado los filtros de seguridad en ambas plataformas: aplicaciones aparentemente inofensivas (camufladas como juegos tipo 'Tetris' o calculadoras) que en realidad buscan acceder al almacenamiento de nuestros móviles para cosechar información sensible con la que chantajearnos o estafarnos.

¿Cómo asegurarnos entonces de que una app aparentemente 'oficial' lo es? Antes de pulsar en 'Descargar' dentro de la 'Play Store' o el 'App Store' debemos atender a las credenciales que figuran en la ficha descriptiva de la aplicación. ¿Quién es su desarrollador? ¿Qué otras aplicaciones ha lanzado hasta la fecha? ¿Cuentan con el suficiente número de valoraciones positivas? En muchas ocasiones, son los propios usuarios quienes alertan sobre el contenido malicioso para evitar que otros piquen. También dudaremos si la app que nos interesa figura como recién publicada y aún no cuenta con reseñas (o apenas dos o tres de cinco estrellas, redactadas en un lenguaje demasiado formal o robótico).

Archivos .apk y webs externas

Lo anterior no quita para que determinadas aplicaciones puedan descargarse a través de las páginas oficiales de sus desarrolladores. Sin embargo, debemos considerar una práctica más que habitual por parte de los ciberdelincuentes: el 'phishing' o la creación de webs de imitación que, con la promesa de ofrecer un producto o servicio, consiguen hacerse con nuestros datos. En el supuesto que nos ocupa, poniendo como ejemplo la descarga de un antivirus para el móvil, podemos toparnos a través del buscador con una web diseñada a imagen y semejanza de la de una compañía de prestigio: el logo, las capturas de pantalla de la app e incluso el tamaño del archivo descargado coinciden con los oficiales, por lo que no nos paramos a sospechar.

Una vez instalado el archivo, sin embargo, comenzaremos a notar que algo no va bien: aunque este tipo de 'malware' suele actuar en segundo plano, existen indicios de infección como que el smartphone u ordenador vaya más lento de lo habitual; que la batería se agote mucho antes, o que aparezcan aplicaciones (en el escritorio o la pantalla de inicio) que no recordamos haber instalado.

Lo anterior también se aplica a los archivos de tipo .apk (instaladores de Android) que solemos encontrar en portales de descarga de aplicaciones. Muchos se presentan como versiones 'beta' o alternativas de WhatsApp, Instagram o TikTok, provistas de ventajas o funciones adicionales que terminan no siendo tales. Al instalarlas nos exponemos no solo a la infección de nuestro dispositivo, también a que el desarrollador original bloquee nuestra cuenta de usuario y, por tanto, perdamos el acceso a nuestro 'feed' de publicaciones o a nuestro historial de chats.

Puestos a instalar una .apk desde un repositorio de apps, mejor hacerlo en una web cuya reputación se encuentre altamente contrastada, como 'APKMirror' o 'F-Droid'. Además, independientemente del lugar donde realicemos la descarga, los expertos recomiendan atender al número de descargas que muestra cada app (en Android, las oficiales suelen superar las 100.000); la dirección web del navegador (si no comienza por 'https', mejor acudir a otra página); y los permisos que solicita en nuestro móvil: ¿Tiene sentido que una app de linterna pida acceso a nuestra ubicación y a la galería de fotos? No, así que algo esconde.

Instalar un programa 'antimalware' y mantener todos los aparatos actualizados a la última versión de su sistema operativo son dos últimos consejos fundamentales que nos ayudarán, primero, a detectar apps de pacotilla, y, segundo, a evitar que estas aprovechen agujeros de seguridad para hacer de las suyas.