

Los mejores tips para detectar apps móviles falsas

Si al descargar un juego móvil, una billetera de criptomonedas, o una app de fitness, la pantalla del teléfono es invadida por publicidades molestas, la aplicación no está haciendo lo que se esperaba, y la cuenta bancaria tiene movimientos que no autorizados, son altas las probabilidades de que la app descargada esté a la búsqueda de dinero o información sensible. ESET, compañía líder en detección proactiva de amenazas, advierte que por la cantidad de información a la que se tiene accesos desde los smartphones, no sorprende por qué los cibercriminales están con un ojo encima de los dispositivos, y siembran grandes cantidades de amenazas, especialmente en tiendas de app de terceros, o no oficiales.

Según el Reporte de Amenazas ESET T3 2022, el número de amenazas en Android se elevó al 57% en los últimos meses de 2022, impulsado por un aumento del 163% en adware y un 83% de aumento en la detección de aplicaciones ocultas.

Lea también: [Meta anuncia mejoras en la supervisión parental en su red social Messenger](#)

Por suerte, se puede evitar tanto el malware como las aplicaciones potencialmente no requeridas (PUAs, por sus siglas en inglés), teniendo cautela. ESET comparte consejos para detectar aplicaciones potencialmente esquivas, así como volver a tener el teléfono “en forma” si ya se ha descargado una de estas aplicaciones.

Cómo reconocer una app falsa

- **Chequear los números:** Si se está buscando una app que se espera que tenga cientos de miles de usuarios, pero se encuentra con una que, aunque suena como la verdadera, no aparece en los rankings como de las más bajadas por los usuarios. Si ese es el caso, las chances de que se esté frente a una app impostora son altas. De hecho, es importante ser precavido siempre que se busque bajar una aplicación popular porque los cibercriminales siempre están deseosos de aprovechar la “fama” de una app o servicio para volcar sus copias falsas en el mercado.

El ejemplo más reciente es una serie de aplicaciones poco confiables que intentaron sumarse a la moda de ChatGPT y fueron lanzadas incluso antes que la aplicación oficial. Lo mismo

aplica a actualizaciones dudosas de aplicaciones ampliamente usadas. Un ejemplo, de 2021, es el curioso caso del WhatsApp Pink un tema de color falso para el servicio de mensajería promocionado vía mensajes en la app.

- Leer las reseñas: Si una app tiene valoraciones negativas de los usuarios, probablemente se debería dejarla pasar. Por otro lado, demasiadas reviews que suenan muy parecidas también podrían levantar sospechas, especialmente aplicaciones que no tuvieron muchas descargas, por lo que esas valoraciones pueden ser falsos usuarios o, incluso, bots.
- Chequear su diseño gráfico: Algo en el color, o el logo de la aplicación que parece no estar bien, si se estás en duda, comparar las visuales con el sitio web oficial del proveedor. Las aplicaciones maliciosas muchas veces imitan a las reales y usan logos parecidos, aunque no idénticos.



De todos modos, no confiar en la falsa sensación de seguridad solo porque se reconozca el logo de un banco reconocido, una billetera de criptomonedas, o un procesador de pagos. Algunas aplicaciones maliciosas no solo usan el nombre de un servicio legítimo, sino que también publican sitios web que son copias idénticas de los sitios legítimos. Mantenerse atento a los detalles -una mirada cercana, que incluya las URL, puede revelar la falsedad-.



- Chequear bien cuando dice “app oficial”: En un caso documentado el año pasado por ESET Research, cibercriminales distribuyeron apps para tiendas online y bancos que no tenían, siquiera, aplicaciones disponibles en Google Play. Cuando se descargue una aplicación móvil que debería estar asociada a un servicio popular, asegurarse de que, en efecto, ofrezcan esa app. Si es el caso, en el sitio oficial se encuentran los links para las tiendas oficiales de Google Play o Apple Store.
- Verificar el nombre y la descripción de la app: Los desarrolladores de aplicaciones legítimas se preocupan por que todo se vea bien profesional. Esto también aplica a cosas mundanas como la descripción de la aplicación -leer en detalle estas para detectar problemas de gramática, o inconsistencias y datos incompletos; pueden dar una idea de que la app no es lo que dice ser.

- Chequear el pedigree del desarrollador: Tener cuidado también cuando se trate de una aplicación de un desarrollador desconocido sin historial en el desarrollo de aplicaciones. Tampoco dejarse engañar por un nombre que suene familiar: los creadores de aplicaciones dudosas pueden estar utilizando indebidamente el nombre de una entidad legítima y conocida. Comprobar si el desarrollador tiene otras aplicaciones a su nombre y si son de buena reputación; en caso de duda, buscar el nombre del desarrollador en Google.
- Prestar atención a si la app pide permisos excesivos: Mantenerse lejos de las aplicaciones que requieren excesivos permisos de usuario, es decir, el tipo de privilegios que realmente no necesitan para hacer su trabajo. Una aplicación de linterna no necesita derechos de administrador ni acceso a las funciones básicas del dispositivo.

Por otro lado, ESET comparte 7 formas de saber si se descargó una aplicación riesgosa:

1. La app no está haciendo su trabajo: Como ejemplo, en 2018 investigadores ESET analizaron aplicaciones que simulaban ser soluciones de seguridad, pero lo que hacían es inundar con publicidad y ofrecer pseudo-seguridad. Estas apps solo imitaban funciones básicas de seguridad con controles de seguridad primitivos que se valían de pocos e intrascendentes códigos genuinos. Como resultado, a menudo detectaban aplicaciones legítimas como maliciosas creando una falsa sensación de seguridad en las víctimas.
- Tiene un comportamiento extraño: ¿La aplicación tiene un comportamiento raro, como abrirse sola, cerrarse, o fallar sin una razón aparente? Este es uno de los signos más obvios de que se puede haber descargado una aplicación dudosa.
 - Tiene cargos inesperados: Si se observan cargos desconocidos en la tarjeta de crédito o la factura del teléfono, podría deberse a la aplicación que descargada recientemente. Como ejemplo, los investigadores de ESET detectaron múltiples apps que simulan ser herramientas de entrenamiento y que abusan de la funcionalidad Touch ID de Apple y roban dinero de los usuarios de iOS. Cuando el usuario abría la app por primera vez, esta le pedía que registre su huella digital con la excusa de “personalizar su seguimiento de caloría y las recomendaciones de dieta”.

Si el usuario tenía una tarjeta de crédito o débito asociada a la cuenta de Apple, el malware podría robar el dinero de las víctimas con pagos fraudulentos en la app.

Pie de imagen: Falsa app iOS pidiendo registro de huellas digitales.

Tener cuidado con las estafas que implican la descarga de un servicio de pago entre pares (P2P) y ofrecen productos y servicios ficticios con descuento. Como los pagos suelen ser instantáneos y no se pueden cancelar, puedes perder dinero pagando por algo que nunca recibirás.

- Mensajes y llamadas desconocidos: Otro signo de que hay problemas tiene que ver con el spam de mensajes que pueden sufrir los contactos. En otros casos, el historial de mensajes y llamadas puede contener registros desconocidos ya que el malware intentará hacer estas llamadas no autorizadas o enviar mensajes a los contactos principales.
- Desgaste de la batería: Si un dispositivo está infectado con malware, este podría consumir los recursos del dispositivo por una excesiva actividad en segundo plano.
- Picos de uso de datos: Si se observa que el uso de datos aumentó sin que se haya tenido cambios en los hábitos de utilización, también podría deberse a una actividad en Segundo plano de una app maliciosa.
- Pop-ups y aplicaciones desconocidas: Una aplicación maliciosa podría instalar otras app adicionales sin tu autorización. Lo mismo ocurre con el adware molesto que muestra publicidades no deseadas. Si se observa alguno de estos, hay altas probabilidades de que deba actuar rápido.

“Cuando descubres una app sospechosa, elimínala, o mejor aún, descarga un software de seguridad móvil de confianza que escanee tu dispositivo y elimine la app. Si quieres ir por la ruta manual, resetea tu dispositivo a la configuración de fábrica –(antes de eso haz el back up de la información). En ocasiones deberás iniciar tu teléfono en modo seguro y así eliminar la app.”, comenta Camilo Gutiérrez Amaya, Jefe del Laboratorio de Investigación de ESET Latinoamérica.

Consejos de ESET para mantenerse protegido:

- Reportar la app en la tienda de la que se la hayas descargado. Se puede también pedir un reembolso de cargos que pueda haberte generado.

- A partir de ahora, si se utilizan aplicaciones de Google Play Store, asegurarse de activar el análisis de Google Play Protect en el dispositivo. También comprobar las aplicaciones que se hayan descargado desde fuera de Google Play Store. Para ello, activar la opción “Mejorar la detección de aplicaciones dañinas”, que enviará automáticamente a Google las aplicaciones desconocidas.
- Limitarse a Google Play y Apple App Store; es decir, evitar ponerse en peligro instalando aplicaciones de tiendas de terceros.
- No hacer clic sin pensar en enlaces enviados a través de mensajes de redes sociales o correos electrónicos.
- Utilizar la autenticación de doble factor (2FA) en todas las cuentas online que la ofrezcan, especialmente en aquellas que contengan datos valiosos.
- Mantener actualizados el sistema operativo y las aplicaciones del teléfono.
- Limitarse a las aplicaciones cuyos desarrolladores sigan mejorando sus productos y corrigiendo las vulnerabilidades de seguridad y los fallos de rendimiento.
- Proteger la pantalla del dispositivo con un código de acceso lo suficientemente largo y complejo o con un elemento biométrico sólido, como la huella dactilar, o, idealmente, con una combinación de ambos.
- Utilizar software de seguridad móvil.

Con información de Descifrado