

EL TIMO DEL TROYANO SUSRIPTOR



Proyecto P-
45 "Audaz"



Buenas a todos ciber-navegantes. Hoy voy a hablaros de un fraude muy común que ocurre en ese aparato del cual no nos podemos despegar prácticamente todo el día: **nuestro móvil**. Y es que, como sabéis, los móviles hoy en día son pequeños ordenadores donde **podemos instalar aplicaciones** que necesitamos, nos hacen gracia o simplemente queremos pasar un rato haciendo algo entretenido. Pero, como en el caso de los PCs, **hay que tener mucho cuidado con lo que se instala**.



💡 **Sí, es peligroso aunque estén en la tienda oficial. Estar en una tienda oficial no te garantiza que la aplicación sea segura, especialmente si es un teléfono Android. Hay indicios para saber cuando algo puede ser o no peligroso (que veremos al final de este documento), pero la seguridad total es muy complicada de tener!**

¿Cuál es el peligro de instalar aplicaciones?

Por tanto, eso de instalar aplicaciones tiene muchos peligros y hoy os voy a hablar de uno de ellos. Su nombre es el **troyano suscriptor**. No se trata de que guerreros de la antigua ciudad de Troya hayan decidido viajar al futuro para ver televisión por internet, sino que es el nombre que reciben una serie de aplicaciones maliciosas (¡y engañosas!) que os podéis encontrar en vuestra tienda oficial del fabricante de vuestro móvil.

💡 **Y esto solo es uno de los tipos de aplicaciones de maliciosas que hay en tiendas, aunque especialmente en la de Android. En la tienda de iPhone hay, pero muchas menos porque hay más control**

Y estas aplicaciones, bajo la apariencia de una aplicación inofensiva o útil, esconden un *malware* qué **os puede hacer perder bastante dinero**. Como veis, el concepto de troyano, porque así se llaman este tipo de aplicaciones, viene del caballo de Troya, donde dentro de algo que aparentemente es inofensivo se esconde vuestro enemigo.

Si pensáis que esta estafa es minoritaria puedo daros datos: por ejemplo, desde el año 2020 se han encontrado 190 aplicaciones infectadas con uno solo de estos troyanos, que se llama *Harly*. Si sumas todas las descargas de estas aplicaciones te da la cifra de casi **5.000.000 de personas** que se lo han descargado e instalado. ¡Y solo estoy hablando de uno de ellos!. Por tanto, proteger tu teléfono es obligatorio, y puedes seguir los consejos del INCIBE (**Figura 1**).

5 consejos para mejorar la seguridad y privacidad en dispositivos móviles



1

Protege el acceso a tu dispositivo

Utiliza contraseñas robustas y mecanismos seguros de desbloqueo



En Ajustes > Seguridad y Ubicación > Bloqueo de pantalla > Contraseña / Huella digital o Smart Lock > Reconocimiento facial.



En Ajustes > Touch ID/Face ID y código.



	PIN	Contraseña alfanumérica	Patrón	Huella dactilar	Reconocimiento facial
Android	✓	✓	✓	✓	✓
iOS	✓	✗	✗	✓	✓



2

Comprueba que tu dispositivo está actualizado ✓



Ajustes > Sistema > Ajustes avanzados > Actualización del sistema.



Ajustes > General > Actualización de software > Descargar e instalar.

3

Haz copias de seguridad y cifra tu dispositivo para salvaguardar tu información



COPIA DE SEGURIDAD

En Ajustes > Google > Hacer copia de seguridad > Crear una copia de seguridad.

CIFRADO

El cifrado se hace por defecto, aunque podemos cifrar una memoria externa en Ajustes > Seguridad y ubicación > Cifrar almacenamiento de tarjeta SD.



iOS

COPIA DE SEGURIDAD

En Ajustes > [nombre] > [seleccionar el dispositivo] > Copia en iCloud > Realizar copia de seguridad ahora.

Al habilitar la opción se realizarán automáticamente.

CIFRADO

El cifrado se hace por defecto.



4

Descarga e instala

Instala aplicaciones seguras desde tiendas oficiales, como Play Store o App Store. Revisa los permisos de las apps descargadas:



Android: en Ajustes > Aplicaciones selecciona la app y haz clic en Permisos para desactivar y activar los que consideres.



iOS: en Ajustes encontrarás las aplicaciones instaladas, selecciona la que quieras y podrás desactivar los permisos.

5

Activa la verificación en dos pasos o doble factor de autenticación. Añade una capa extra de seguridad a tus cuentas



Ajustes > Google > Gestionar tu cuenta de Google > Seguridad > Verificación en dos pasos > Empezar.



iOS 10.3 O SUPERIOR:

Ajustes > [nombre] > Contraseña y seguridad > Activar autenticación de doble factor > Continuar.

iOS 10.2:

Ajustes > [Apple ID] > Contraseña y seguridad > Activar autenticación de doble factor > Continuar.

Recuerda que ponemos a tu disposición la Línea de Ayuda en Ciberseguridad de INCIBE, 017, gratuita y confidencial, para cualquier cuestión relacionada con la ciberseguridad.

www.incibe.es | www.osi.es



GOBIERNO
DE ESPAÑA



VICEPRESIDENCIA
TERCERA DEL GOBIERNO
MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN
E INTELIGENCIA ARTIFICIAL



INSTITUTO NACIONAL DE CIBERSEGURIDAD



017



Oficina
de Seguridad
del Internauta



@INCIBE @osiseguridad

Figura 1. Consejos de protección de móviles del INCIBE. Fuente: <https://www.incibe.es/ciudadania/blog/protege-tu-movil-ios-y-android-con-5-consejos>

¿Y cómo funciona este tipo de troyanos suscriptores?

Bueno, lo primero que tienes que entender es cómo se crea un troyano. Hay dos formas:

- **Creándolo directamente**, porque los delincuentes tienen la capacidad técnica de hacer programas para teléfonos móviles. Hacen un programa aparentemente útil, lo publicitan de alguna forma y dentro esconden el código realmente dañino.

 **Esta aplicación puede incluso hacer lo que promete para que la “tapadera” sea más efectiva**

- **Descargándose una aplicación legítima y manipulando su código**. Los delincuentes tienen la capacidad técnica y las herramientas necesarias para meter dentro de una aplicación existente código malicioso. Cuando ya han hecho ese “gemelo malvado”, vuelven a subirla a la tienda como una copia o una versión de la aplicación original.

 **En otras palabras, lo que estamos viendo probablemente sea un clon de algo que realmente existe, creado por alguien que solo quiere ganar un poco de dinero vendiendo su aplicación. Pero su trabajo acaba de ser aprovechado por un grupo criminal para hacer un clon maligno de la misma. Como comprenderéis, esto también es un perjuicio para el autor original de la aplicación, que no tiene nada que ver, no sabe nada, pero se llevará un más que probable impacto a su reputación 😞.**

Se cree de una forma u otra, hay **indicios claros** de que estás ante una aplicación troyanizada, con este efecto malicioso u otro cualquiera. Estos son:

- Te encuentras con una aplicación conocida, pero con una **versión Plus o Premium** de la que no has oído hablar nunca, y si vas a la web de su fabricante no la menciona. Probablemente sea un clon alterado maliciosamente de la original que se llama así para llamar tu atención. En este caso el autor de la versión debe ser **exactamente el mismo** que la aplicación original para que sea algo legítimo.
- Te encuentras con **una versión gratuita** de una aplicación o juego de pago. A veces existen (es una versión con menos características de la original o una demo), pero eso te lo tiene que decir la web del fabricante. Si no te lo dice, es un fraude seguro. En este caso el autor de la aplicación debe ser **exactamente el mismo** que el de la versión de pago para que sea algo legítimo.
- Aplicaciones con un **nombre o ícono muy parecido** a una conocida: Están jugando al despiste, y al clic por error, lo que es un indicio de ser algo malicioso.
- Aplicaciones que **prometen demasiado** (publicidad agresiva, cosas imposibles como más RAM, más espacio en el teléfono, resolver problemas de velocidad o batería...).

 **Es muy frecuente encontrar “aplicaciones milagro” que realmente son maliciosas. Hay que hacer una inspección detallada antes de instalarlas, de la que hablaremos luego.**

¿Y qué me puede pasar?

Una vez que ejecutas esta copia maliciosa de la aplicación original, la aplicación **recopila toda la información que pueda** sobre tu teléfono y sobre tu proveedor de red móvil. Hecho esto, se conecta a la red móvil y **te suscribe** a una serie de servicios de pago que obviamente tú no has

pedido, con lo cual ahora mismo adquieres el **compromiso de pago** de cosas que ni conoces ni quieres.

Alguna gente me dice que cómo es esto posible, si cuando te suscribes a un sitio muchos servicios te envían un mensaje o te piden que llames a un número de teléfono. Estos delincuentes saben bien lo que hacen, y el propio troyano suscriptor **es capaz de recibir el mensaje o hacer la llamada que se necesita sin que tú te enteres**, ni por supuesto tengas que hacer nada.

Y esto, en otras palabras, consiste en que tienes contratado algo de forma fraudulenta que te hace perder dinero y obviamente ganarlo a los delincuentes. Si un delincuente consigue infectar y cobrar durante al menos un mes a un gran número de dispositivos, al final va a obtener un beneficio considerable.

🔍 *Y a ti, que te darás cuenta cuando te llegue la factura, no te va a quedar otro remedio de meterte en el complicado proceso reclamar a la operadora, denunciar la estafa, y esperar a ver si es posible recuperar el dinero que te han robado.*

Y, además, esto es como lo que he dicho otras veces: muchas veces el dinero que te han robado es una cantidad baja y por esas cantidades uno no se toma la molestia de denunciar. Lógicamente el atacante lo sabe, y se aprovecha de eso para seguir con sus actividades.

🔍 *Por supuesto, ten en cuenta que estamos hablando solo de un tipo de troyano: el suscriptor. Los hay bancarios (roban los datos de tu cuenta o aplicación del banco y la usan en tu nombre), extorsionadores (te piden dinero por recuperar tus datos o no publicar datos privados), espías...y muchos otros tipos. Pero todos pueden atacarnos de la forma que veremos en la sección siguiente.*

¿Y qué podemos hacer para defendernos de esto?

Lo primero, **no poner fe ciega en los programas antimalware** porque, aunque ayudan a protegerte, no son infalibles. Tener o no uno dependerá de la capacidad de tu móvil, de la frecuencia con la que instalas aplicaciones y, en general, del uso que hagas del mismo. La **Figura 2** muestra como debes descargártelo y, sobre todo, actualizar tu teléfono (si aún es posible) para evitar ser víctima de problemas de seguridad que se vayan descubriendo con el tiempo que estas aplicaciones puedan aprovechar.

PRIMEROS PASOS PARA MEJORAR LA SEGURIDAD

4 PROTECCIÓN CONTRA VIRUS Y FRAUDES

Antivirus / Actualización de software

Antivirus:

Tu dispositivo no está exento de riesgos de infectarse por algún virus a través de una app o al descargar un archivo infectado. Para protegerlo:

- Selecciona un antivirus directamente desde la tienda oficial [Play Store](#), asegurándote de que previamente lees las reseñas de este.
- Haz clic en **Obtener**. Es posible que tengas que iniciar sesión con tu ID de Google.
- Abre la app y configúrala para mantener tu dispositivo Android libre de virus

Disponible en [Google Play](#)

Actualización de software:

Durante la vida útil del sistema operativo, los desarrolladores van descubriendo errores y fallos de seguridad que necesitan ser solucionados. Sin actualizaciones, tu dispositivo estaría más expuesto y vulnerable frente a los ataques de los ciberdelincuentes.

- Si no has recibido la notificación de que existe una actualización nueva o quieres revisar si está actualizado o no, dirígete a **Ajustes > Información del teléfono > Actualizaciones del sistema/software > Comprobar actualizaciones** y comprueba si tienes la última versión.

Otras herramientas de protección:

Además de con antivirus, blinda [el acceso a tu información](#) con aplicaciones de bloqueo de apps, gestores de contraseñas, función de verificación en dos pasos o que protegen tu privacidad, entre otras.

incibe_
 017
 Oficina de Seguridad del Informante

[Más información](#)

GUÍA DE DISPOSITIVOS MÓVILES | 06/12

Figura 2. Antivirus y actualizaciones son una primera línea de defensa. Fuente: <https://www.incibe.es/sites/default/files/docs/guia-seguridad-android.pdf>

Programas antimalware para móvil hay muchos, gratuitos y de pago. Para ayudarte a elegir, tienes este artículo: <https://www.xatakandroid.com/listas/9-mejores-antivirus-gratis-para-movil>, del que sale la **Figura 3**.

<p>AVG Antivirus Gratis AVG Mobile</p> <p>★★★★★</p>	<p>Antivirus & Eliminar TAPI Security Labs (Anti)</p> <p>★★★★★</p>	<p>Antivirus, Antimalware Kaspersky Lab</p> <p>★★★★★</p>	<p>ESET Mobile Security ESET</p> <p>★★★★★</p>	<p>Protección Malware Malwarebytes</p> <p>★★★★★</p>	<p>Security Antivirus - Power Both App Inc.</p> <p>★★★★★</p>
<p>Avast Antivirus Gratis Avast Software</p> <p>★★★★★</p>	<p>Bitdefender Antivirus Bitdefender</p> <p>★★★★★</p>	<p>Super Security: Elim DUALSPACE studio</p> <p>★★★★★</p>	<p>Antivirus Android Security Systems Lab</p> <p>★★★★★</p>	<p>Nox Security-Antivirus Nox Ltd.</p> <p>★★★★★</p>	<p>Safe Security - Antivirus Safe Security Develop</p> <p>★★★★★</p>

Figura 3. Una selección de los mejores antivirus para Android según Xataka

Pero la principal medida de seguridad es **instalar programas con cabeza**, es decir, desarrollar y usar un **sentido común** a la hora de hacerlo. No instales cualquier cosa, y si lo vas a hacer, cumplir con una serie de normas:

- Que sea de un **editor/autor recomendado o conocido**. Puedes visitar su página web para saber quién es, con quien colabora, a qué se dedica...

🔍 ¿No te suena de nada? Para eso está la Wikipedia 😊

- Que tenga **buenas valoraciones**, normalmente por encima de 4 estrellas (**Figura 4**). Un mal ejemplo puedes verlo en la **Figura 5**.
- Que tenga **muchas descargas**, ya que si hace algo malo alguien lo habrá notado, y cuanta más gente lo use más probable es que lo haga (**Figura 4**). Un mal ejemplo puedes verlo de nuevo en la **Figura 5**.
- Pero, sobre todo, **fíjate en los comentarios de los usuarios**. Es muy frecuente que muchas de las personas que han “caído en la trampa” dejen una reseña avisando al resto de usuarios de que el programa tiene “bicho”. Fíjate por ejemplo en lo que indican los comentarios de la **Figura 6**.



Figura 4. Una aplicación de Android que cumple con todos los indicios de ser legítima: Autor conocido (Mozilla es una fundación muy popular), buenas valoraciones (y muchas), muchas descargas...

Revenge Classic Birds VKL

Davidhome

Compras directas desde la app

2.9★

318 opiniones

50 k+

Descargas

E

Apto para todo público ⓘ

Instalar

Compartir

Agregar a la lista de deseos

Figura 5. Una aplicación de Android que NO cumple con todos los indicios de ser legítima: Autor desconocido (es un particular), malas valoraciones, pocas descargas...y encima admite compras dentro de la aplicación (posibles compras accidentales)

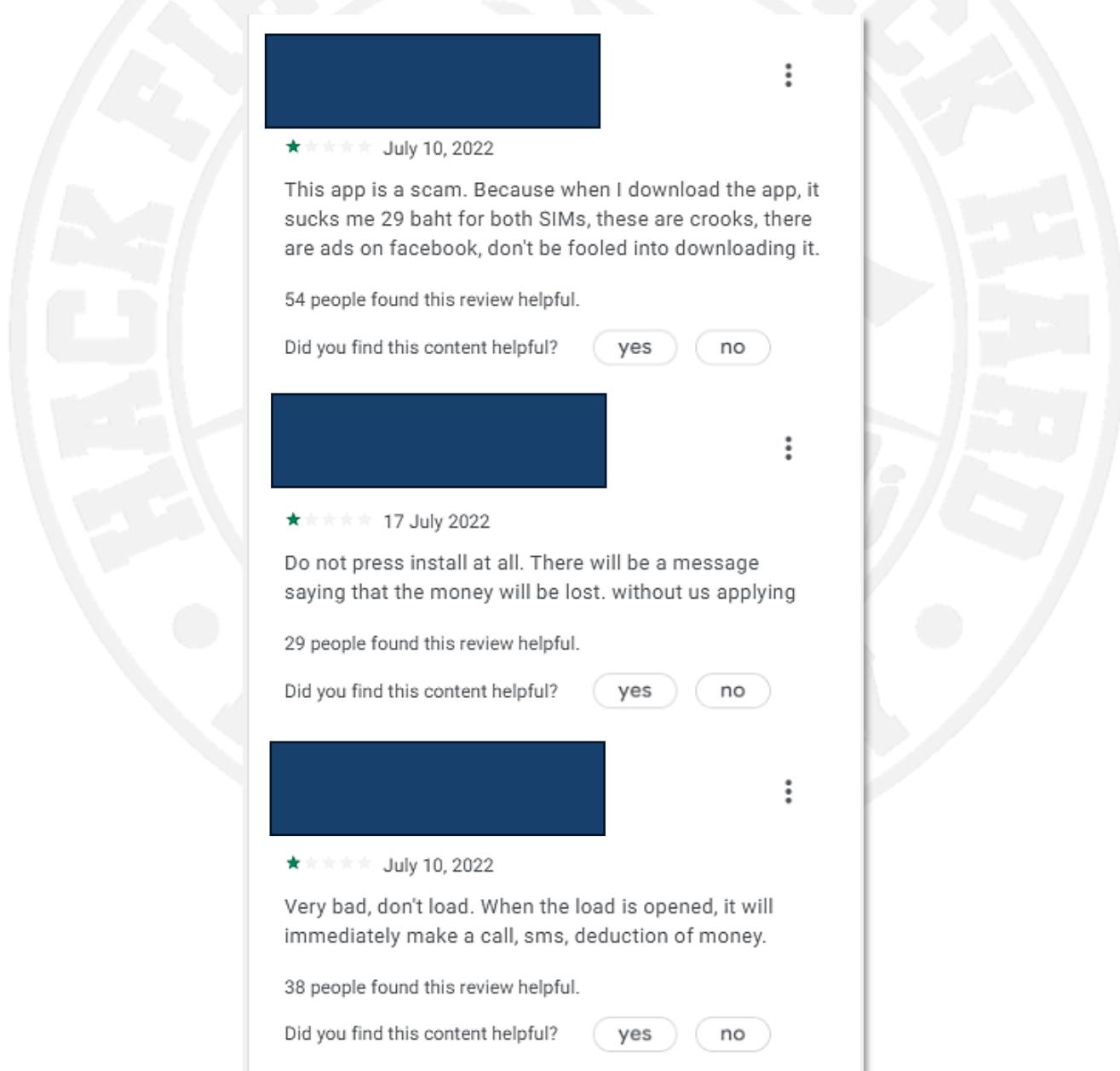


Figura 6. Comentarios que indican que aplicación es maliciosa. En este caso fíjate que precisamente indica que es un troyano suscriptor como el de este artículo

Finalmente, además de todo lo dicho a la hora de vigilar de cerca todo lo que instalamos y hacerle una “ficha policial” antes de hacerlo, la **Figura 7** recoge una serie de consejos del INCIBE para mantener tu móvil a salvo de estos troyanos (suscriptores o de otro tipo) en nuestro día a día.

PRIMEROS PASOS PARA MEJORAR LA SEGURIDAD ✓

9 CONSEJOS GENERALES

- 1 Vincula tu dispositivo móvil a una [cuenta Google](#) en tu móvil Android.
- 2 Utiliza una clave de bloqueo para tu dispositivo. Si no es biométrica, recuerda usar una [contraseña robusta](#).
- 3 Activa el sistema de [actualizaciones automáticas](#) de tu dispositivo y aplicaciones, pues con esto se corrijen los defectos en seguridad que puedan tener.
- 4 Usa [aplicaciones de seguridad](#) que añadan una capa extra de seguridad a tu dispositivo, como por ejemplo un antivirus.
- 5 Protege tu información mediante [copias de seguridad](#). De este modo tendrás una copia de respaldo en caso de pérdida o borrado de tu dispositivo.
- 6 Desactiva las conexiones inalámbricas una vez hayas terminado de usarlas (wifi, Bluetooth, NFC).
- 7 Cuando instales aplicaciones, [revisa siempre quién es el desarrollador así como las opiniones y valoraciones del resto de usuarios](#). ¡Y acuérdate de Google Play [eliminar las que ya no uses!](#)
- 8 [Otorga los permisos a las apps que sean imprescindibles](#) para su correcto funcionamiento y revisa siempre que sean coherentes con la funcionalidad de la app.
- 9 [Evita prácticas de riesgo](#) con el rooting en Android.
- 10 Si vas a deshacerte de tu móvil, [asegúrate de borrar toda la información](#) que contiene para no dejar rastro.
- 11 Apóyate en [herramientas de control parental](#) si el dispositivo lo va a utilizar un menor.

GUÍA DE DISPOSITIVOS MÓVILES | 11/12

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD 017 OSi Oficina de Seguridad del Internauta

Figura 7. Consejos generales para la protección de móviles

Y finalmente un poco lo de siempre. Por favor, **cuéntaselo a la gente** porque esto es algo que no sabe mucha gente, y nunca sabes cuando alguien que conozcas puede instalar lo que no debe. **¡Que corra la voz!**

¡Y esto es todo! Muchas gracias y... ¡nos vemos en la próxima entrega!

Y recuerda amigo/a, ¡que una aplicación esté en una tienda oficial no significa que esté libre de todo mal!



¿Quieres escuchar como hablo de esta estafa en menos de 5 minutos?



1

- [Escúchalo en IVOOX](#)
- [Escúchalo en Amazon Podcast](#)
- [Escúchalo en mi canal de YouTube](#)
- [¿Tienes otro cliente de Podcast? Este es el feed RSS](#)

¿Quieres leer alguna noticia/artículo relacionado?



- [Harly: otro troyano suscriptor en Google Play \(28/09/2022\)](#)
- [El peligroso troyano que te suscribe a servicios de pago y ya ha infectado a millones de móviles \(07/10/2022\)](#)
- [Malware WAP. Como te suscriben a servicios de pago los troyanos suscriptores](#)
- [Troyano bancario Brokewell: qué es, cómo te roba tus datos bancarios y cómo evitarlo \(01/05/2024\)](#)
- [Ojo con las suscripciones y los pagos a terceros que engordan tu factura telefónica \(19/03/2022\)](#)

Este documento usa material generado con IA²

¹ Audio emitido en "Más de Uno". 95.2 Onda Cero Oviedo (<https://www.ondacero.es/emisoras/asturias/oviedo/directo/>) el 15/05/2023

² Algunas imágenes del texto del documento han sido generadas con la IA Bing Chat