

EL TIMO DE LAS NOTIFICACIONES FALSAS



Proyecto P-
45 "Audaz"



Buenas a todos ciber-navegantes. Voy a hablaros de un “truco” que los delincuentes hacen cada vez más en páginas web: **Poner notificaciones falsas o engañosas**. Aunque ser víctima de esto es relativamente fácil de prevenir, estas notificaciones son cada vez más creíbles y sofisticadas, y es necesario hablar con detalle de ellas.



🔍 *Básicamente te muestran algo en pantalla que parece una ventana del sistema operativo o un aviso importante. Siempre con algo alarmante y preocupante. ¿El objetivo? Que hagas clic en él. Y, desgraciadamente, luego pasan cosas 😞*

¿En qué consiste ese truco?

Una de las cosas que las páginas web modernas pueden hacer es mostrarnos avisos variados encima de su contenido. Esto, en principio, se usa mayoritariamente para **anuncios, promociones o advertencias** de diferentes tipos: el mecanismo no es en sí algo malo. El problema es cuando se usan en este tipo de elementos **para engañar**. ¿Como? Pues hay varias técnicas, que casi siempre cumplen con lo siguiente:

- **Copiar el aspecto de algo “oficial”**. Normalmente estas notificaciones funcionan si son creíbles, y hay un trabajo detrás para que parezcan genuinas, de programas o compañías legítimas conocidos (*Windows, Apple, Google, Microsoft, distintos antivirus...*luego veremos algunos ejemplos)
- Siempre hay una **sensación de urgencia** a la hora de la actuar, normalmente recurriendo al miedo y a la coacción (tienes virus, tu equipo está en riesgo...)
- Son muy **intrusivos** (ocupan toda la pantalla) y llamativos

Es un método tan hoy día común que **hay muchos tipos y modelos**. A continuación veremos unos cuantos para que seas capaz de identificarlos si te encuentras con uno.

🔍 *Algo que suele funcionarle a la gente para entenderlos es tratarlos como si fuesen emails. Hazte a la idea de que estas notificaciones son como si recibieras un email de un desconocido con el mismo contenido. La gente empieza ya a desconfiar de emails así por lo general, pero por alguna razón (supongo que porque a veces los “cuelan” como publicidad en páginas legítimas, como hablaremos luego) en los anuncios no parecen desconfiar tanto. Pues hazlo: un anuncio no tiene más valor que un email. Puede ser 100% falso*

La forma en la que aparecen suele ser muy común. Seguro que esto te resulta familiar:

- Entras a una página web y, de pronto una ventana aparece ocupando gran parte del área visible. Te pide que des un “Me gusta” a su página en una red social, te suscribas a algo, te registre...o cualquier otra cosa para seguir viendo el contenido de la web
- Tras unos segundos leyendo alguna noticia o artículo, aparece un aviso notificando una promoción de un producto o servicio que ofrece la web o uno de los anunciantes que han pagado por poner ahí su publicidad (ver **Figura 1**).

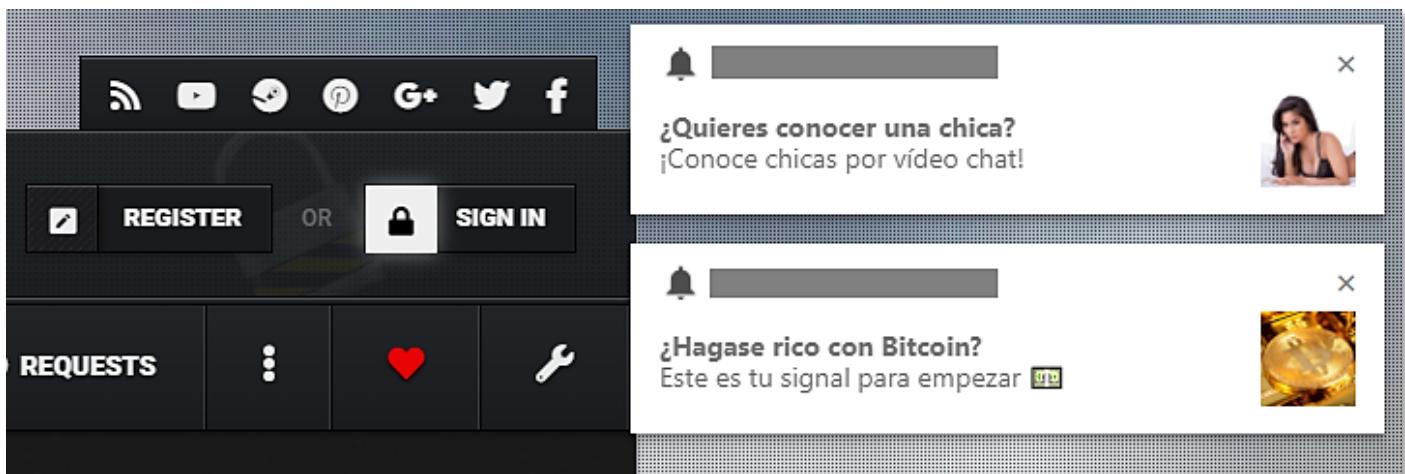


Figura 1. Ejemplo de notificación de una web. Como ves el contenido nada tiene que ver con la web en sí, son reclamos publicitarios (con bastantes probabilidades de ser algo fraudulento). Fuente: <https://www.incibe.es/ciudadania/blog/que-significan-los-mensajes-y-notificaciones-que-aparecen-al-navegar-por-internet>

A continuación vamos a ver una serie de ejemplos de estas notificaciones clasificadas por lo que intentan hacer. La mayoría están en inglés, por lo que te voy a decir qué ponen por si no lo entiendes. Pero hazte a la idea de que existen por toda Internet un **equivalente a cada una de ellas en Español**. ¡No saber inglés no te libra de este problema! 😊

Y olvídate también de que estén mal redactadas: ¡Con los avances en IA esto cada vez pasa menos!

Notificaciones que te invitan a llamar a un teléfono

Son notificaciones que buscan una excusa como las que hemos mencionado **para que llames tú a un teléfono**, diciéndote que así van a solucionarte un problema (que se inventan, por supuesto). Aunque las excusas para que lo hagas encajan en otras categorías muchas veces, aquí hemos agrupado las que te muestran el teléfono al que llamar directamente.

Un ejemplo famoso son las alertas de Microsoft de virus pornográficos. Esta falsa ventana emergente parece bloquear el dispositivo debido a la “navegación por sitios web pornográficos no seguros”. La ventana emergente da un número de teléfono que lleva a una estafa de soporte técnico, que intenta venderle un falso software antivirus para “desbloquear” tu ordenador. En realidad tomarán control de él 😞

Insisto que en los ejemplos aparecen teléfonos americanos, pero **existe un equivalente con teléfonos españoles**. Detrás puede haber incluso un locutorio organizado con personas contratadas para estafar a los que llamen. Nunca dudes de que estos delincuentes pueden tener montado algo profesional. Puedes ver ejemplos en la **Figura 2**, la **Figura 3** y la **Figura 4**.

 Y el teléfono encima es gratuito! Qué generosos! 😊



Figura 2. Tienes muchos virus en el PC, llama a este teléfono que te lo solucionamos. Fíjate como usan logos de programas reales para engañar.
Fuente: <https://malwaretips.com/blogs/remove-virus-alert-warning-popup/>

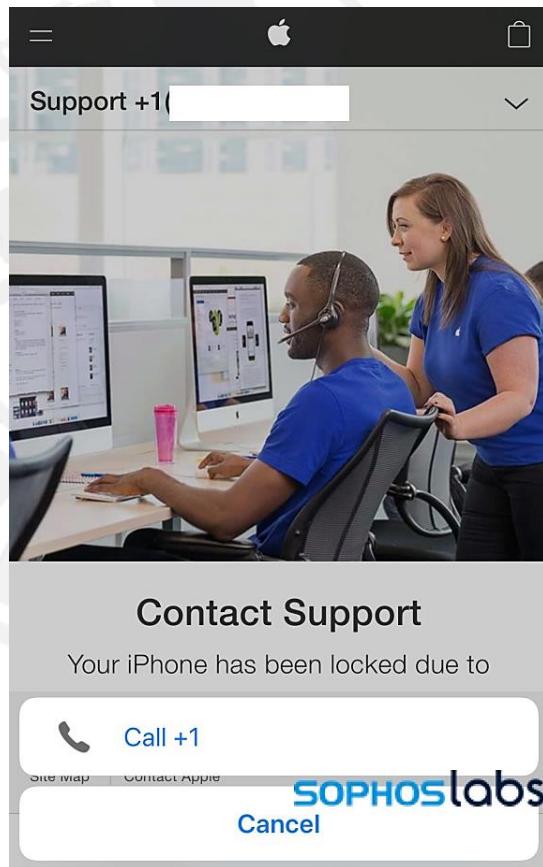


Figura 3. Un aviso de que contactes con un falso soporte técnico porque tu teléfono ha sido supuestamente bloqueado por algún motivo. Fuente: <https://news.sophos.com/es-es/2020/09/10/alertas-falsas-como-detectarlas-y-detenerlas/>

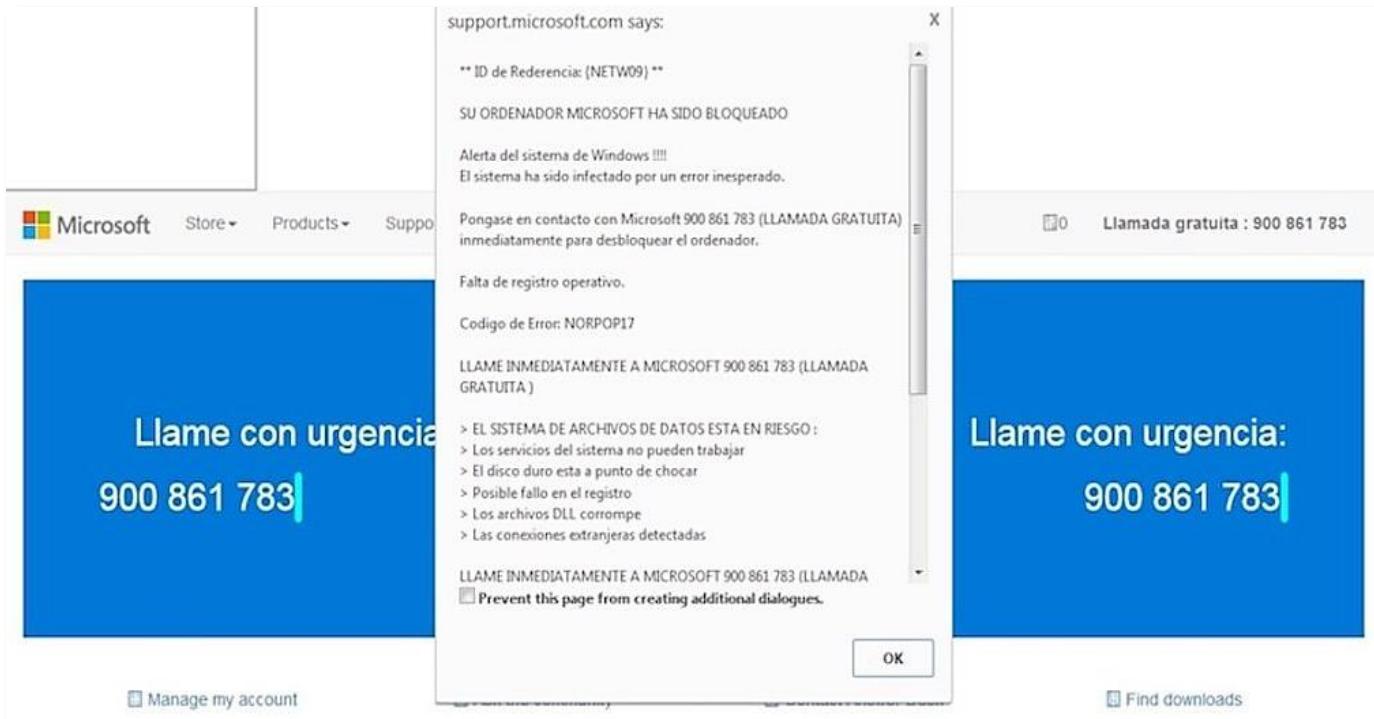


Figura 4. El timo de Microsoft "a la inversa" (que llames tú en lugar de que te llamen ellos) es una estafa que normalmente empieza con una notificación fraudulenta. Fuente: <https://www.tuexperto.com/2020/06/26/has-recibido-una-llamada-de-microsoft-cuidado-puede-ser-un-timo/>

Descargas de programas fraudulentos

Las notificaciones fraudulentas son una vía muy típica para engañar a la gente y **que se descarguen programas**, usando el gancho de ser una oferta, tener funcionalidades interesantes, estar (falsamente) creados o patrocinados por alguien fiable, necesitarlos para hacer alguna tarea cotidiana, o algo así. Estos programas pueden luego causar a la víctima a un buen nº de problemas, como por ejemplo:

- **Troyanos:** Programas que funcionan, pero que dentro además tienen *malware* que hace alguna clase de ataque
- **Programas falsos:** Supuestos antivirus, limpiadores de PC, etc. que realmente no hacen su función. Lo que si hacen es algo que beneficia al creador (venta de datos de uso, robo de información...)
- **Programas que roban directamente datos:** Tus cuentas, contraseñas, datos bancarios, información privada...
- **Secuestradores de PCs:** Para usar tu PC para cometer delitos o extorsionarte para recuperarlo. El ***ransomware*** es uno de los más típicos
- **Documentos:** Que pueden estar infectados con cualquiera de los efectos anteriores

La **Figura 5**, **Figura 6** y la **Figura 7** muestran ejemplos de estos avisos.

 **Como ves, al final no es más que una treta para que te descargues software que, de otra forma, no descargas**

The screenshot shows a search results page from a search engine. At the top, there are navigation links for Dictionary, Thesaurus, Word Dynamo, Quotes, Reference, Translator, and Spanish. Below these are links for 'The Hot Word', 'Daily Crossword', 'Word Games', 'Writing Dynamo', 'Crossword Solver', 'Tools', and 'Mobile'. The main content area displays several search results, each with a snippet of text and a small image. One result is from 'HOME 18 SHOP.com' about cameras, another from 'EmblemHealth' about health coverage, and others related to grammar and language. On the left, there's a sidebar with a 'Word of the Day' (bollix - to do something badly; bungle), a 'Grammar Checker' section with a 'Try now!' button, and social sharing icons for Facebook, Twitter, and Pinterest.

Figura 5. Doble anuncio para descargarte cosas: Un documento (que podría estar infectado) y un comprobador de gramática y sintaxis de dudosa procedencia. Fuente: <https://www.incibe.es/ciudadania/blog/que-significan-los-mensajes-y-notificaciones-que-aparecen-al-navegar-por-internet>

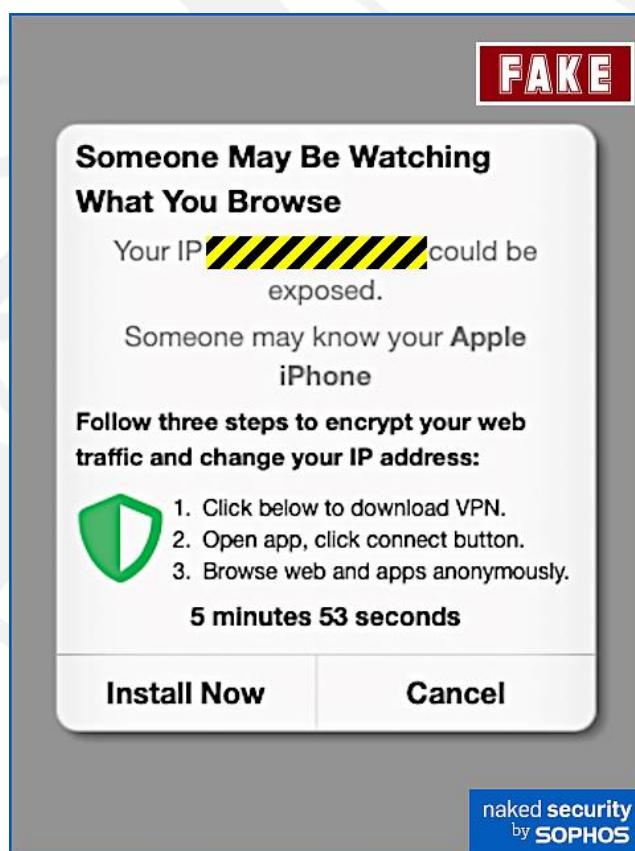


Figura 6. Anuncio diciendo que te están espiando y te invita a descargar un supuesto software VPN que te "protege". En realidad es un malware. Fíjate que encima te mete prisa...Fuente: <https://news.sophos.com/es-es/2020/09/10/alertas-falsas-como-detectarlas-y-detenerlas/>

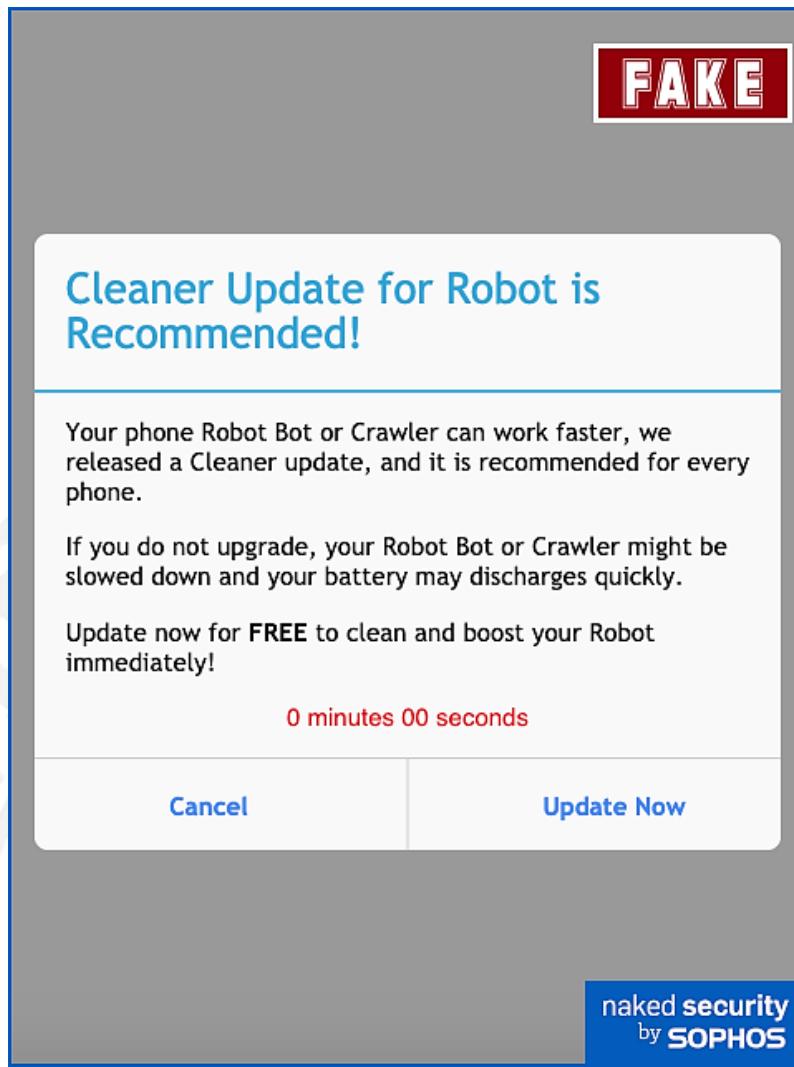


Figura 7. Aviso falso para que instales una nueva versión de un programa, que es un malware realmente. Aquí vemos el componente de prisa y amenaza de que el software va a dejar de funcionar bien. Fuente: <https://news.sophos.com/es-es/2020/09/10/alertas-falsas-como-detectarlas-y-detenerlas/>

Falsas actualizaciones

Una variante de la anterior son las **notificaciones de falsas actualizaciones de programas**. Es el mismo tipo de aviso fraudulento para que te descargas software seguramente malicioso, pero en este caso la excusa siempre es la misma: uno de tus programas necesita actualizarse para seguir trabajando normalmente o algo similar. **Todo es, evidentemente, falso**. Pero, al ser quizá una de las formas más comunes de encontrarse con este problema, he decidido hacerle una sección aparte.

💡 **Normalmente en estos casos el programa que necesita actualizarse es el navegador**

Como puedes ver en la **Figura 8**, la **Figura 9** y la **Figura 10**, las notificaciones se adaptan perfectamente al navegador con el que estás viendo la página, cambiando logos y versiones.

💡 **Un navegador se actualiza automáticamente salvo que tú le hayas dicho expresamente que no lo haga, así que ¡olvídate de estas notificaciones, son todas falsas!**

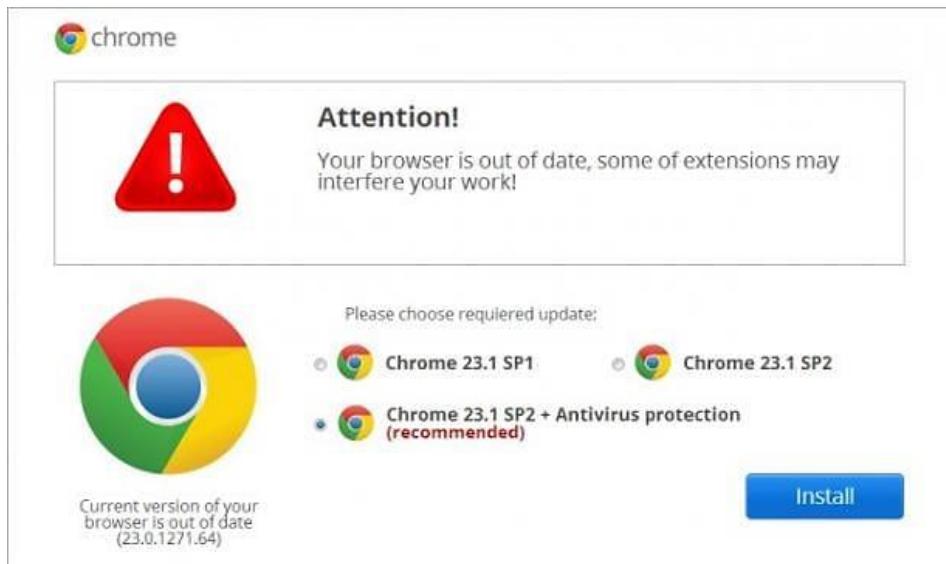


Figura 8. Una supuesta actualización para Chrome. Fuente: <https://www.geektopia.es/es/technology/2012/11/29/noticias/un-nuevo-malware-presenta-notificaciones-falsas-para-actualizar-el-navegador-incluso-en-iphone.html>



Figura 9. La misma notificación cuando navegas en la misma página usando Firefox. Que curioso que siempre necesitas actualizar el navegador, sin importar cual usas...Fuente: <https://www.geektopia.es/es/technology/2012/11/29/noticias/un-nuevo-malware-presenta-notificaciones-falsas-para-actualizar-el-navegador-incluso-en-iphone.html>



Figura 10. Las notificaciones también detectan si estás navegando por móvil o PC para adaptarse a quien visita la web que las muestra. Fuente: <https://www.geektopia.es/es/technology/2012/11/29/noticias/un-nuevo-malware-presenta-notificaciones-falsas-para-actualizar-el-navegador-incluso-en-iphone.html>

Falsas infecciones por virus

Es una de las notificaciones fraudulentas más comunes y, si tienes dudas acerca de cómo distinguir cuando una de ellas es falsa, puedes seguir estas normas:

- **Se recomiendan productos desconocidos.** Instalar un antivirus requiere que te informes de los más comunes, y nunca instalar productos que no tienen referencias o valoraciones en páginas conocidas
- **Alertas demasiado frecuentes:** Una ráfaga de avisos de virus es alarmante. Pero se trata de una táctica de este tipo de avisos maliciosos muy común. El objetivo es ponerte lo suficientemente nervioso como para que descargues el producto falso
- **Errores gramaticales:** Una empresa real se toma tiempo para pulir sus mensajes y comunicaciones. Pero no uses esto como un criterio definitivo, la IA está eliminando las barreras de idioma
- **Se detectan muchos virus:** Si recibes alertas de que el ordenador tiene varias infecciones de *malware*, es muy probable que se trate de un engaño para provocar el pánico. Si el aviso te sale dentro de una web, no le hagas caso
- **Solicitudes de dinero instantáneas:** Si una notificación de que tienes un virus pide dinero por resolver la infección, es falsa
- **Redacción ambigua:** Las promesas ambiguas o las descripciones vagas de los productos son muy sospechosas
- **Dispositivos lentos:** A veces, una falsa alerta de virus lanzará una nueva ventana detrás de la ventana de su navegador. Si el dispositivo se ralentiza repentinamente o escuchas los ventiladores del ordenador haciendo mucho ruido, es posible que tengas un tipo de notificación maliciosa de las que tratan de colapsar el sistema

La **Figura 11**, la **Figura 12**, la **Figura 13** y la **Figura 14** muestran avisos de esta clase.

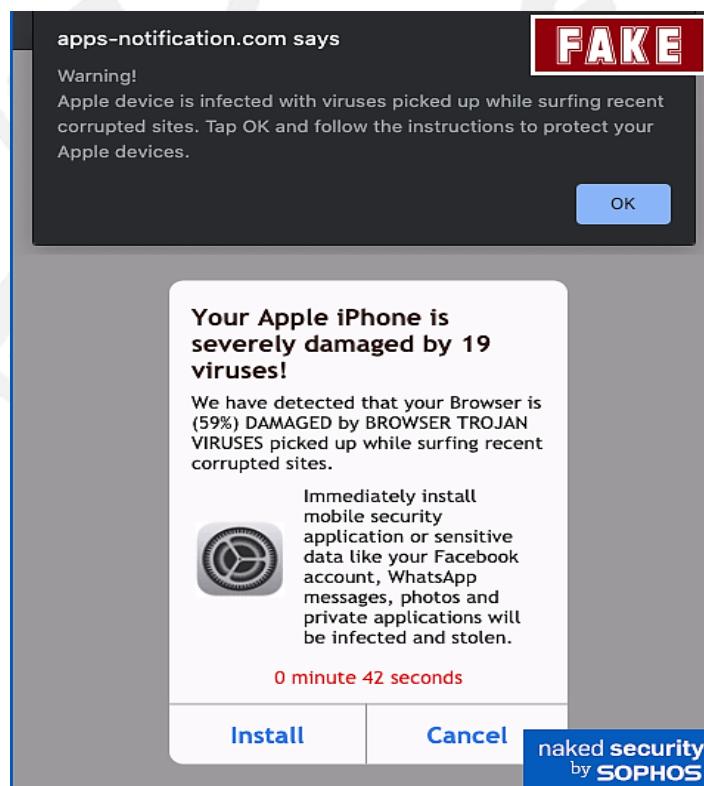


Figura 11. Nada menos que 19 virus y usando el sistema de notificaciones del teléfono además. Todo falso. Fuente: <https://news.sophos.com/es-es/2020/09/10/alertas-falsas-como-detectarlas-y-detenerlas/>



Figura 12. Otra infección masiva (¡15 virus!), y encima con componente de prisa para provocar el pánico y que piques. Todo mentira. Fuente: <https://www.avg.com/es/signal/spot-fake-virus-warning>



Figura 13. "Solo" 5 virus, pero fíjate en las tremendas consecuencias que tienen. De nuevo el miedo como elemento para que piques e instales lo que ellos quieran. Todo falso. Fuente: <https://www.avg.com/es/signal/spot-fake-virus-warning>

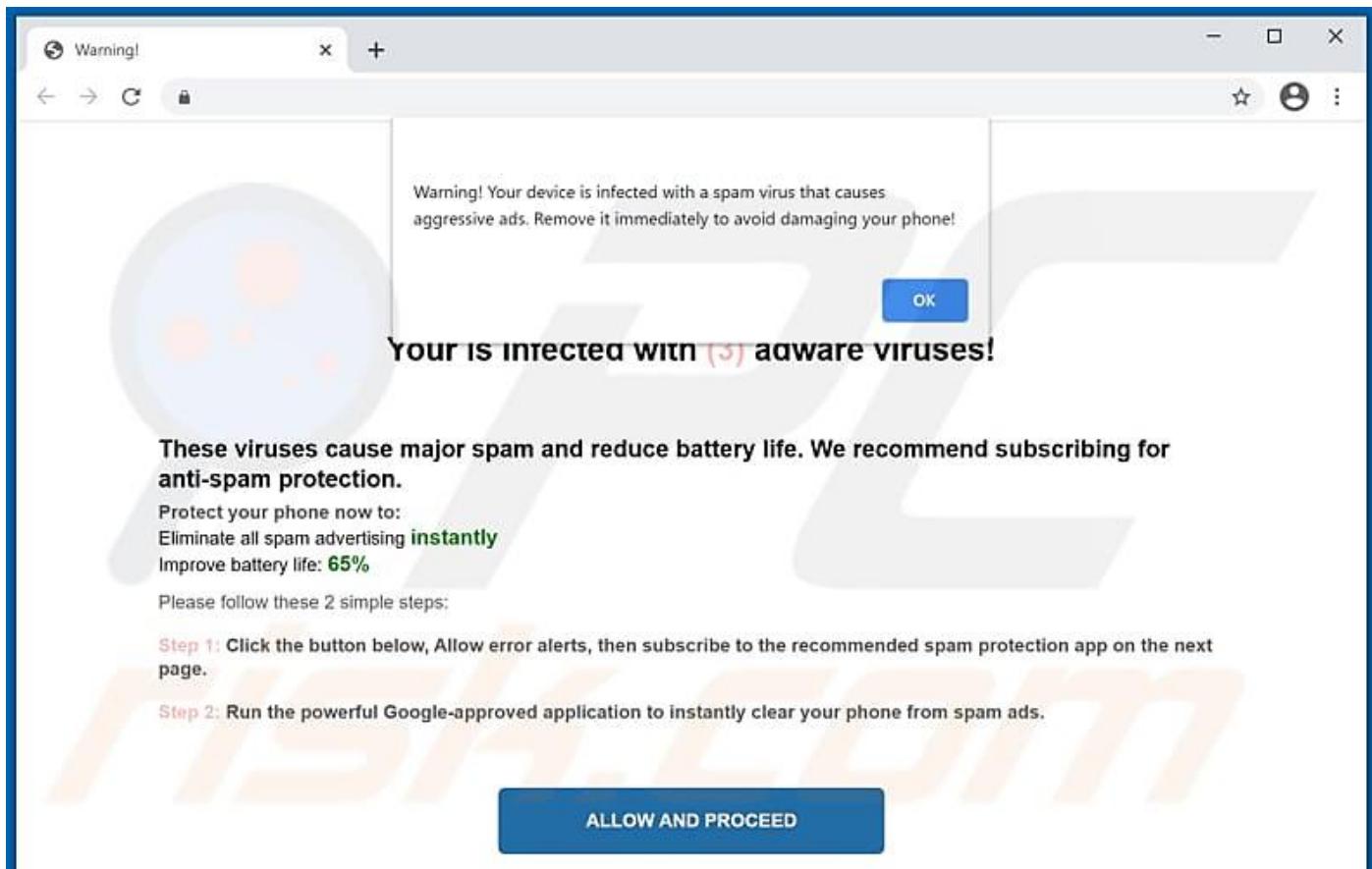


Figura 14. Un aviso similar en un navegador de PC, prometiendo a demás casi magia cuando instalas el producto y suplantando a Google. Fuente: <https://www.pcrisk.es/guias-de-desinfeccion/10641-your-device-is-infected-with-a-spam-virus-pop-up-scam>

Notificaciones integradas en Windows

Las notificaciones de la bandeja del sistema son más raras que otros avisos de virus falsos. Aparecen en la bandeja del sistema como notificaciones que te informan de un problema que requiere una acción inmediata. Son especialmente peligrosas por lo convincentes que parecen, ya que aunque las envían los navegadores parecen genuinas de tu sistema operativo. La Figura 15 muestra un ejemplo de ellas. Antes de interactuar con cualquier notificación, debes asegurarte de que es auténtica.

No obstante, luego veremos que se pueden desactivar, de forma que el navegador nunca podrá enviarte algo así. Es algo que conviene hacer, hay muy pocas razones para permitir a un navegador ponerte notificaciones en esa parte del SO

Al igual que otras formas de falsos avisos ya vistos, puedes comprobar si estas notificaciones son reales examinando el lenguaje. Estas estafas **siempre utilizan un lenguaje “emocional”** para asustarte y engañarte y que tomes decisiones precipitadas



Figura 15. Una notificación en Windows enviada por un navegador. Por favor, desactívalas porque mayoritariamente solo traen disgustos. Fuente: <https://support.microsoft.com/es-es/microsoft-edge/administrar-notificaciones-de-sitios-web-en-microsoft-edge-0c555609-5bf2-479d-a59d-fb30a0b80b2b>

No obstante, aunque desactives estas notificaciones los delincuentes es común que acaben haciendo anuncios que **copian los colores y la letra de una ventana de Windows**. Dentro de ella se coloca en un aviso alarmante de un problema o un error que debes solucionar, junto con una solución, como en los casos ya vistos. Pero por el aspecto parece algo de *Windows* aunque salta del navegador.

El malvertising

Es una de las fuentes de notificaciones falsas más común. El *malvertising* ocurre cuando las **redes publicitarias legítimas se infectan con anuncios maliciosos** que luego pueden aparecer en sitios web en los que habitualmente se confía. Dicho de otra forma, tú por ejemplo estás navegando por tu periódico habitual y te sale un anuncio del estilo de lo que hemos visto (habitualmente de infecciones de *malware*). Ignóralos.

Otra variante son los **anuncios falsos de empresas legítimas**, cuando el anuncio parece provenir de una empresa de confianza (usando logos, colores, tipos de letra, etc. usados por anuncios reales de dicha empresa) pero realmente dirigen a una página falsa.

 **En definitiva: No hagas clic en los anuncios. Hay tantas posibilidades de que sean falsos ¡que lo mejor es evitarlos todos!** 😊

La consecuencias

¿Y qué pasa si me descargo lo que me dicen?

No creo que haga falta describir mucho qué pasa si te descargas un programa recomendado por este tipo de anuncios: **te habrán colado un software malicioso** que puede hacer lo que quieran con tu PC: robarte toda tu información privada, usar tu PC para propagar más malware, ... O en definitiva cualquier cosa que a ellos les dé un beneficio a costas tuya. Lo mencionamos anteriormente

¿Y si en lugar de eso me dice de ir a una web?

Imagina que estás navegando por internet y haces clic en un enlace o anuncio que parece inofensivo. Sin saberlo, podrías acabar siendo víctima de un ataque de **drive-by download**. Este tipo de ataques funcionan así:

- **Engaño:** El atacante crea un sitio web o anuncio malicioso que parece legítimo
- **Explotación de vulnerabilidades:** El sitio web aprovecha vulnerabilidades en tu navegador o sistema operativo para ejecutar código malicioso en tu dispositivo
- **Descarga silenciosa:** Sin que te des cuenta, se descarga *malware* o *software* no deseado en tu dispositivo

 *El peligro es que no pocas veces podrá ejecutarlo sin que tú hagas nada. Y sí, esto significa que es posible que simplemente por navegar por una web te encuentres infectado por un virus. ¡Razón de más para tomar las medidas que veremos luego!*

- **Toma de control:** El *malware* puede tomar control de tu dispositivo, robar información personal, instalar otro *software* malicioso o incluso cifrar tus archivos para pedir un rescate

¿Bueno, pero, cierro y listo, no?

Si bien las alertas falsas móviles y las páginas similares en los navegadores de escritorio se pueden cerrar fácilmente, las páginas fraudulentas de soporte de “bloqueo del navegador” a menudo usan *scripts* que hacen que sea difícil o imposible cerrar el navegador web o navegar por otras páginas, incluyendo:

- Forzar la ventana del navegador al tamaño de pantalla completa.
- Ocultar o camuflar el cursor del ratón.
- Lanzamiento de descargas de archivos sin fin.
- Aparición de cuadros de inicio de sesión que solicitan un nombre de usuario y una contraseña.
- Intentar capturar las pulsaciones del teclado para evitar la navegación fuera de la página con atajos de teclado.

Usar el *Administrador de tareas* (en *Windows*) o *Forzar salida* (en *MacOS*) pueden ser la única forma de escapar de algunas de estas páginas. Otra opción es reiniciar y no permitir que el navegador restaure las páginas de la última sesión.

Vale, pero entonces ... ¿Cómo lUCHO contra esto?

La principal medida para luchar contra este tipo de problemas es **nunca hacer caso a un aviso que nos dé una página web**. Aunque pueda ver alguno que sea legítimo, la plaga de avisos maliciosos que existe hace que sea mejor no fiarnos de ninguno. Y, por supuesto, hay que mantener el navegador actualizado y si buscas un poco desactivar la acción de mostrar notificaciones en las páginas web que tienen muchos navegadores. Si necesitas medidas preventivas más concretas, puedes usar esta lista como guía:

- **Ten cuidado con lo que haces clic:** No hagas clic en enlaces o anuncios sospechosos, incluso si provienen de personas que conoces
- **Mantén tu software actualizado:** Instala las últimas actualizaciones de tu sistema operativo, navegador y software de seguridad
- **Usa un antimalware:** Instala y actualiza un *antimalware* de confianza para protegerte

- **Desactiva scripts y plugins innecesarios:** Desactiva los scripts y *plugins* que no uses en tu navegador para reducir la superficie de ataque.
- **Ten cuidado con las descargas:** Descarga *software* solo de sitios web oficiales y confiables.
- **Utiliza una red Wi-Fi segura:** Evita usar redes Wi-Fi públicas no seguras para navegar por internet.
- **Instala un bloqueador de anuncios** en nuestro navegador
- **Desactiva las notificaciones** del navegador
- **Bloquea las ventanas emergentes** en el navegador
- **Desactiva las notificaciones** de las aplicaciones en dispositivos móviles

¿Cómo hacer todo esto? Por suerte el INCIBE, como parte de su iniciativa “**Programa Senior**”, que recomiendo mucho leer y consultar, tiene documentado cómo hacerlo en todos los navegadores más comunes. Puedes consultarlos aquí:

<https://www.incibe.es/ciudadania/blog/que-significan-los-mensajes-y-notificaciones-que-aparecen-al-navegar-por-internet>

Y recuerda:

- **La prevención es la mejor defensa:** Tomar medidas preventivas te ayudará a evitar ser víctima de un ataque de *drive-by download*
- **Mantente informado:** Estar al día sobre las últimas amenazas y vulnerabilidades te ayudará a protegerte mejor
- **No tengas miedo de pedir ayuda:** Si sospechas que tu dispositivo ha sido infectado, consulta a un experto en seguridad informática o al **teléfono 017 del INCIBE**: <https://www.incibe.es/linea-de-ayuda-en-ciberseguridad>



Servicio gratuito y confidencial, disponible de 08:00 am a 11:00 pm los 365 días del año.

TU AYUDA EN CIBERSEGURIDAD



017

Teléfono
017



900 116 117

WhatsApp
900 116 117



@INCIBE017

Telegram
@INCIBE017



Formulario web



Atención presencial

 Financiado por la Unión Europea
NextGenerationEU

 GOBIERNO DE ESPAÑA
 MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y LA FUNCIÓN PÚBLICA
 SECRETARÍA DE ESTADO DE DIGITALIZACIÓN Y ARTIFICIAL INTELIGENCIA

 Plan de Recuperación, Transformación y Resiliencia
 INSTITUTO NACIONAL DE CIBERSEGURIDAD

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, lo mejor es nunca hacer clic en ningún anuncio.
¡Salga en donde te salga!**



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

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



1

¿Quieres leer alguna noticia/artículo relacionado?



- [Así puedes eliminar los mensajes de virus de Chrome \(10/05/2023\)](#)
- [Alertas falsas: cómo detectarlas y detenerlas \(10/09/2022\)](#)
- [Falsos avisos de virus: Cómo detectarlos y evitarlos \(12/09/2022\)](#)
- [¿Qué es la estafa "Your device is infected with a spam virus?" \(26/07/2021\)](#)
- [Un nuevo malware presenta notificaciones falsas para actualizar el navegador, incluso en iPhone \(29/11/2012\)](#)
- [¿Qué significan los mensajes y notificaciones que aparecen al navegar por Internet? \(01/09/2021\)](#)

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 22/05/2023

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