'Malvertising', cuando la publicidad es peligrosa. Google retiró 5.100 millones de anuncios maliciosos en 2024. Y a veces no hace falta ni hacer clic...

J. C. CASTILLO

ILUSTRACIÓN **ADOBE STOCK**

Entrar a cualquier web o aplicación supone toparnos con una cascada de anuncios, en muchos casos, abrumadora. A veces se trata de inserciones publicitarias inofensivas (cuyo objetivo es que compremos), pero también las hay diseñadas expresamente para causarnos problemas. Son anuncios maliciosos. Esto último es lo que los expertos en ciberseguridad denominan 'malvertising'. Pueden aparecernos, incluso, mientras navegamos por sitios web de nuestra plena confianza. Y no nos hacen sospechar que al hacer clic sobre el 'banner' o la ventana emergente terminaremos infectando nuestro dispositivo.

«Desde la perspectiva de un 'hacker', el 'malvertising' es un modo relativamente fácil de comprometer sitios que reciben mucho tráfico, pero sin tener que atacarlos directamente», explica Oliver Buxton, especialista de la firma antivirus Avast. El experto también describe esta práctica como una amenaza dinámica: «Los ataques más sofisticados pueden infectar aunque no se haga clic en los anuncios maliciosos gracias a que esconden códigos –dentro de imágenes de unos pocos píxeles– imperceptibles para los mecanismos de control».

El primer ataque de 'malvertising' registrado se remonta a 2007, cuando unos ciberdelincuentes aprovecharon una vulnerabilidad de Adobe Flash para colar programas maliciosos en sitios por entonces muy populares, como la red social MySpace. La amenaza no ha dejado de crecer desde entonces: solo en 2024, Google retiró 5.100 millones de anuncios maliciosos, presentes en 1.300 millones de páginas, y suspendió las cuentas de más de 39 millones de anunciantes.

Operadores telefónicos que no lo son

La mayoría de los ataques de 'malvertising' –hasta un 81% durante el cuarto trimestre del año pasado, según el informe de la firma AdMonsters– se corresponden a redireccionamientos forzados. Un ejemplo: nos aparece un anuncio invitándonos a descargar un conocido antivirus gratuito y, al pinchar, somos redirigidos a una web diseñada a imagen y semejanza de la oficial, donde descargaremos un ejecutable capaz de acceder a la información de nuestro móvil. En ocasiones puede que la descarga se aloje automáticamente en la carpeta al efecto, sin clic alguno por nuestra parte. Otras fórmulas habituales de 'malvertising' son las estafas de soporte técnico, prosigue Buxton. «Los anuncios fraudulentos suelen instalar algún tipo de 'malware' de secuestro del navegador para perturbar la experiencia del usuario y, después, le indican que llame a un número de teléfono para resolver este problema inexistente», relata. Es entonces cuando los estafadores (siempre haciéndose pasar por empleados de una gran empresa tecnológica) intentan que hagamos pagos innecesarios mediante tarjeta de crédito.

También abunda el 'scareware', que son anuncios alarmantes, con mensajes de error que invitan a descargar un programa capaz de resolverlos en segundos; las promesas de ingresos sin esfuerzo rellenando encuestas que en realidad permiten a terceros tomar el control de nuestro ordenador; y las falsas actualizaciones que inundan los gadgets con 'software' espía. En estos casos conviene recordar que los errores y la disponibilidad de actualizaciones del sistema operativo siempre se nos notificarán mediante ventanas del propio sistema, nunca al abrir el navegador o acceder a webs externas.

> «Los anuncios fraudulentos suelen instalar algún 'malware' de secuestro del navegador»

Los niños, especialmente vulnerables

En el contexto de la publicidad en internet, los niños resultan especialmente vulnerables. Los de menor edad pueden terminar pinchando en 'banners' fraudulentos por el colorido; y los adolescentes, picar en la falsa promesa de descuentos o contenido adicional gratuito para sus videojuegos.

Por esto mismo, el Incibe aconseja a los padres desactivar la publicidad personalizada en aquellas redes sociales que lo permitan (dentro de sus apartados de configuración); instalar bloqueadores de anuncios y pautar unos tiempos de uso máximo.

Además, deberíamos enseñarles a navegar de forma responsable, mostrándoles qué espacios de internet resultan de confianza y cuáles se encuentran libres de publicidad. Lo habremos hecho bien si vemos que, al toparse con un anuncio en el móvil o la tablet, toman por costumbre cerrarlo. Y es que, como ocurre con mucho de lo que vemos y leemos en la red, mejor desconfiar por norma de todos los avisos, ofertas y oportunidades que nos asaltan a diario entre signos de exclamación.

Busca 'click-to-play' en tu navegador

Además de no pinchar en aquellos anuncios que consideremos sospechosos para combatir el 'malvertising', el Instituto Nacional de Ciberseguridad (Incibe) recomienda mantener todos nuestros dispositivos actualizados para contar con los últimos parches de seguridad; instalar y habilitar únicamente aquellos complementos de navegador que resulten indispensables para el día a día; adoptar un software de seguridad con detección de virus, 'malware' y 'spyware'; actualizar programas como Java o Adobe desde sus sitios oficiales; y habilitar la función 'click-to-play', disponible en la mayoría de navegadores. Al hacerlo, deberemos permitir la ejecución de cualquier 'plugin' que intente iniciarse al visitar cualquier web.