L·A·M·A·C
LATIN AMERICAN MULTICHANNEL ADVERTISING COUNCIL

Noticias sobre TV Paga

5 Datos de Marketing sobre Tráfico Inválido en Publicidad Digital

Las malas prácticas en la distribución de publicidad en los sitios web y el tráfico inválido (fraude), generan grandes pérdidas para los anunciantes y sus marcas.

25/07/2019

Las malas prácticas en la distribución de publicidad en los sitios web y el tráfico inválido (fraude), generan grandes pérdidas para los anunciantes y sus marcas.

El tráfico inválido es una forma fraudulenta de incrementar la cantidad de visitas a un sitio web con la intención de incrementar su costo por click/impresión o bien para rankearse más alto en los inventarios de compra programática. El aumento del tráfico inválido afecta negativamente a los anunciantes y agencias, pues su campaña jamás llegará al público objetivo o jamás será visto.

En ese sentido, una impresión no visible, ¿debe considerarse como una impresión válida? La respuesta es un rotundo “no”. Después de todo, si un anuncio no es visto, entonces no puede ser posible que haga su trabajo: lograr un impacto en el consumidor.

A continuación, te presentamos 5 datos sobre el Tráfico Invalido y Fraude Publicitario que refuerzan la importancia de asociar a las marcas con medios y canales de comunicación que cuenten con procesos rigurosos altamente controlados, lo cual garantiza a los anunciantes que su reputación no está en riesgo, dado que el 100% de sus anuncios están inmersos en un contexto confiable y seguro.

1. Tipos de tráfico no válido

Los anunciantes necesitan que el tráfico sea de alta calidad para que sus campañas sean un éxito. Los estafadores lo saben, por lo que la mayoría de las formas de fraude implican convertir el tráfico no válido en algo que parezca legítimo. Sin embargo, no todo el tráfico inválido es necesariamente fraude.

Tráfico General Invalido

El tráfico general invalido incluye el tráfico generado por rastreadores y bots conocidos. Este tráfico no intenta imitar el comportamiento humano y no se considera fraudulento. Ejemplos: tráfico proveniente de Data Centers, bots autoidentificados, rastreadores de motores de búsqueda y tráfico de proxies.

Tráfico Invalido Sofisticado

El tráfico invalido sofisticado es un tráfico fraudulento que busca aparecer como legítimo. Este tráfico evita patrones simples que puedan identificarse fácilmente y pueden representar una amenaza grave para la calidad del tráfico. Ejemplos: Bots que imitan el comportamiento humano, dispositivos hackeados, adware/malware, anuncios ocultos y/o apilados, tráfico de proxies fraudulento.

Fuente: www.programaticaly.com – Blog: El fraude en la publicidad digital, 2019

2. Fraude que afecta a los Anunciantes

Anuncios Apilados

Varios anuncios se apilan uno encima del otro, pero solo hay un anuncio visible (superior). Sin embargo, todos los anuncios se pagan, independientemente de si son visibles o no.

Suplantación de Aplicación

Una App "falsa" es capaz de enviar un identificador falso a los anunciantes para hacerles creer que es una aplicación premium (o la real). Los anuncios aparecen en una aplicación diferente a la que el comprador tenía previsto anunciarse, lo que afecta de lleno a la seguridad de la marca (Brand Safety). Es decir, el anunciante está comprando un inventario premium que no lo es y a cambio está recibiendo espacios en aplicaciones de baja calidad.

Tráfico en segundo plano

Un código malicioso es capaz de generar tráfico cuando la aplicación está en segundo plano o cuando el smartphone ni siquiera se está utilizando. Esta aplicación inactiva "muestra" anuncios que no serán vistos por los usuarios.

Bots

Los bots, pueden ser desde simples a muy sofisticados, y suelen usarse para una variedad de actividades maliciosas, como generar tráfico, clicks o instalaciones falsas.

Clicks fraudulentos

Suelen ser bots maliciosos o "granjas de clicks" que generan dinero proveniente de los anunciantes que pagan más por espacios publicitarios con altas tasas de clicks o que pagan por click. Otra forma de fraude es la inyección de clicks, en la cual Apps de Android (normalmente con permisos excesivos) activan un click antes de que se complete la instalación de una nueva aplicación. Los "estafadores" reciben dinero por la instalación quitándoselo directamente al anunciante.

Fraude de Retargeting

Los bots imitan el comportamiento de clientes interesados (por eso el retargeting) para atraer un mayor número de eCPM's en todas las Apps que participan en el fraude.

3. Fraude que afecta a los Usuarios

Descargas automáticas

Un anuncio engañoso provoca una descarga automática sin la intención del usuario. El elemento descargado es a menudo malicioso.

Redireccionamientos automáticos

Los redireccionamientos automáticos llevan a los usuarios a páginas que se parecen a sitios web conocidos pero que se usan para instalar malware o robar datos confidenciales. Más comúnmente, estos redirigen automáticamente a los usuarios a una tienda de aplicaciones, con el fin de lograr un mayor rendimiento.

Minas de criptomoneda

Los anuncios contienen un código JavaScript para minar criptomonedas sin que el usuario lo sepa. Los estafadores ganan dinero, mientras que los smartphones de los usuarios ven cómo el rendimiento de su teléfono se ve afectado y su batería agotada.

Malware

Los estafadores sirven un anuncio que hace que un usuario descargue un programa dañino. Se puede usar malware para robar datos (por ejemplo, phishing), bloquear las funciones de las teclas del smartphone o incluso bloquear el dispositivo. El malware puede incluso utilizarse para generar tráfico de anuncios fraudulentos.

VAST Arbitrage

Al servir anuncios de video in-banner, un DSP (demand-side platform) puede revender de manera fraudulenta una impresión de video ganada en un espacio de anuncios de Display. Si pueden revenderlo por más de lo que inicialmente pagaron, tienen la garantía de ganar dinero. Si no pueden revenderlo, el anuncio registrará un error y el DSP no tendrá que pagar.

4. El fraude publicitario cuesta billones a la industria

Según el IAB, el fraude publicitario le cuesta a la industria $ 8.2 mil millones al año solo en los EE. UU. Los estafadores han encontrado formas de jugar con el sistema y ganar dinero al publicar anuncios de manera que ninguna persona real pueda verlos. No hace falta decir que esto tiene un efecto negativo en toda la comunidad publicitaria.*

Fuente: Integral Ad Science, World Federation of Advertisers/Compendium of ad fraud, knowledge for media investors

5. El fraude publicitario tiene enormes implicaciones financieras y éticas

La Federación Mundial de Anunciantes (WFA) estima que el Fraude Publicitario superara los 50 mil millones de dólares para 2025.

Por cada $3 dólares gastados en publicidad digital, $1 dólar se desperdicia en Fraude.

Después del tráfico de drogas, el fraude publicitario es el segundo mas grande crimen organizado a nivel mundial.

Fuente: WFA Article, WFA issues first advice for combatting ad fraud, 2016 – COULL.com