Compendio sobre el fraude publicitario para inversores en medios

Coautores: WFA y
THE ADVERTISING FRAUD COUNCIL

Mikko Kotila
Director, botlab.io
mailme@mikkokotila.com

Ruben Cuevas Rumin
Profesor auxiliar, UC3M
rcuevas@it.uc3m.es

Shailin Dhar
Consultor independiente especializado
en fraude publicitario
adtechexpert@gmail.com

WFA WORLD FEDERATION OF ADVERTISERS

Compendio sobre el fraude publicitario para inversores en medios

ÍNDICE

ACERCA DE ESTE DOCUMENTO

La intención de este compendio es concienciar a los propietarios de marcas sobre el fraude publicitario y proporcionar la información y las prácticas adecuadas para contrarrestarlo de manera eficaz. Este documento pretende animar a los propietarios de marcas a adoptar estas prácticas y a colaborar con los socios del sector con vistas a introducir los cambios necesarios para reducir considerablemente el fraude.

Este documento ha recibido el apoyo de los miembros del Global Transparency Group de la WFA y ha sido aprobado por los miembros del **MEDIA**FORUM y el **CDO**FORUM de la WFA.

Para las tareas de creación, recopilación de datos e investigación que hay detrás de esta guía, la WFA ha contado con el apoyo de Botlab.io, una fundación que se dedica a investigar el fraude publicitario, las violaciones de los derechos de los usuarios y otras prácticas maliciosas en la cadena de suministro de la publicidad online.

Este documento solo pretende servir como orientación; no debe considerarse una guía exhaustiva. Su objetivo es proporcionar consejos generales para ayudar a los miembros de la WFA a la hora de tomar decisiones unilaterales sobre sus operaciones internas y externas con los medios digitales.

Publicado en 2016

Compendio sobre el fraude publicitario para inversores en medios

RESUMEN EJECUTIVO

- El fraude publicitario representará probablemente más de **50 000 millones de dólares en 2025, incluso según las previsiones más conservadoras**. Sin las medidas suficientes para contrarrestarlo, se puede prever fácilmente un panorama en el que los ingresos del fraude publicitario asciendan a 150 000 millones de dólares al año en el mismo intervalo de tiempo.
- Prácticamente **todas las compras programáticas están expuestas al fraude publicitario**. Se debería desconfiar de cualquier afirmación que asegure lo contrario.
- Los sitios de *spam* viral, que ofrecen pocas o ninguna oportunidad de eficacia publicitaria, son endémicos en Internet. Pero el fraude publicitario también tiene lugar entre los editores premium, por ejemplo en forma de tráfico comprado. **La compra de tráfico de poca calidad se ha convertido en algo frecuente entre los editores, que a menudo lo utilizan para alcanzar los objetivos de campaña de los anunciantes**.
- El fraude publicitario es obra de varios actores. A pesar de ello, **el principal beneficiario no intencionado del fraude publicitario es la industria del marketing**.
- **Los anunciantes son los que más pierden con el fraude publicitario** y, si no se toman medidas eficaces, los problemas relacionados con esta amenaza seguirán creciendo tanto en alcance como en complejidad.
- No existe ninguna panacea que solucione este problema; de hecho, es muy posible que siga habiendo **un porcentaje de exposición al fraude publicitario de hasta el 10 % por muchas medidas que se tomen**.
- Hasta que el sector pueda demostrar que es capaz de afrontar el fraude publicitario, **los anunciantes deberían ser prudentes en lo que respecta a aumentar su inversión en medios digitales** si quieren limitar su exposición al fraude.
- **Los anunciantes pueden realizar diversas medidas para mejorar la situación**, ya sea establecer nuevas normas, introducir cambios en los contratos, exigir más transparencia y dedicar recursos internos a contrarrestar el fraude publicitario.
- **Se necesita un cambio de conducta en todo el sector**, que solo se puede conseguir mediante el entendimiento y la motivación adecuados y un enfoque común.

"El fraude publicitario es uno de los problemas más importantes al que nos enfrentamos hoy en día. Nos comprometemos a continuar el diálogo para fomentar la toma de conciencia y crear soluciones. Esperamos que esta guía ayude al sector a identificar las oportunidades y soluciones posibles, tanto para los anunciantes como para los propietarios de medios y las empresas de tecnología".

Benjamin Jankowski,
Director de Medios Globales de MasterCard y Presidente del MEDIAFORUM de la WFA

Compendio sobre el fraude publicitario para inversores en medios

¿QUÉ ES EL FRAUDE PUBLICITARIO?

Por definición, el fraude publicitario se asocia a una actividad en la que las impresiones, los clics, las acciones o los eventos de datos se falsean para obtener ingresos de manera ilegal o con otros propósitos fraudulentos o maliciosos. Las actividades de fraude publicitario con la intención de generar ingresos son las más comunes, pero la creación de ruido y otras actividades que no generan ingresos también están presentes en el ecosistema actual de la publicidad en Internet.

En resumen, hay cuatro tipos de fraude publicitario:

1. fraude de impresión
2. fraude de clics
3. fraude de conversión
4. fraude de datos

En todos estos casos, los informes validan una visita como auténtica cuando en realidad es fraudulenta. Estas visitas fraudulentas pueden ser totalmente mecánicas, humanas o una mezcla de ambas.

¿CUÁL ES LA MAGNITUD DEL PROBLEMA DEL FRAUDE PUBLICITARIO?

Cuando los investigadores estiman la exposición al fraude publicitario en porcentajes tan dispares como un 2 %[1] y un 90 %, queda claro que no hay ningún medio disponible en gran medida para evaluar el índice de exposición total. El reto que supone establecer esa cifra queda de manifiesto con los recientes descubrimientos de investigación de la WFA, que demuestran que el 36 %[2] de los encuestados afirman no saber hasta qué punto están expuestos al fraude publicitario.

Una de las iniciativas de investigación más destacadas sobre el fraude publicitario ha sido el reciente informe "Bot Baseline"[3] dirigido por la ANA, la asociación nacional de anunciantes de EE. UU. En este informe se estima el coste del fraude publicitario en 7200 millones de dólares, lo que equivale aproximadamente al 5 % de la totalidad del mercado de medios digitales en todo el mundo.

Aunque esta es sin duda una cifra muy significativa, una investigación primaria llevada a cabo por Botlab.io junto con sus colaboradores académicos y otros terceros (de la cual se proporcionan muestras a continuación), sugiere que la magnitud del problema podría ser aún mayor:

- se estima que el 88 % de los clics en anuncios digitales son fraudulentos [4]
- los editores de medios digitales encabezan todos los sectores en cuanto a tráfico de *bots* maliciosos con un 32 % [5]
- los *bots* inflan las audiencias rentables desde un 5 % hasta un 50 % [6]
- el tráfico de *bots* supone hasta un 61,5 % de todo el tráfico web [7]
- una única forma de fraude en aplicaciones supone el 13 % de todo el inventario [8]
- el tráfico de *bots* fraudulentos crece un 22 % respecto al año anterior [9]
- el 40 % de los clics en la publicidad móvil son básicamente inútiles [10]
- el tráfico de *bots* alcanza por primera vez más del 50 % del total [11]
- más del 18 % de las impresiones/clics proceden de *bots* [12]

Compendio sobre el fraude publicitario para inversores en medios

El propósito de este informe no es llevar a cabo más investigaciones empíricas para cuantificar el valor que representa el fraude publicitario hoy en día. Sin embargo, para promover el cambio en nuestro sector, resulta útil plantear la posible magnitud actual del problema y la que podría llegar a alcanzar en el futuro, de acuerdo con distintos escenarios.

A lo largo de este documento se han tenido en cuenta dos escenarios: un índice de exposición global relativamente conservador del 10 % y un valor más alto del 30 %. Otros estudios ya realizados por terceros y la investigación primaria llevada a cabo por Botlab.io y sus colaboradores dejan claro que la cifra real podría ser superior al 30 %.

Cabe subrayar que el fraude publicitario no solo se manifiesta en forma de tráfico de *bots*, sino también como otras formas de actividad fraudulenta (descritas brevemente en este informe), por lo que el índice global total de exposición al fraude publicitario será mayor que el porcentaje que representa el tráfico de *bots* en el tráfico total.

El coste real del fraude publicitario supera con creces los ingresos que genera. Un estudio global en curso desarrollado por Deloitte y la WFA, y proyectos similares elaborados por la AA, la asociación de publicidad del Reino Unido[13], demuestran que por cada dólar que se pierde debido a la falta de eficacia de la publicidad, se pierde hasta 6 veces más en términos del negocio. Los daños causados por el fraude publicitario se pueden resumir en:

1. el coste para la eficacia del marketing;
2. el coste para el negocio (y para la categoría de negocio);
3. el coste para la economía nacional (y el contribuyente).

Esto significa que, cuando se ataca la eficacia de la publicidad de un anunciante determinado, la economía nacional a la que contribuye dicho anunciante también se ve afectada. En este sentido, el fraude publicitario plantea un nuevo riesgo de seguridad, ya que proporciona una forma de atacar la economía de un país determinado.

> *"Como anunciantes, tenemos la responsabilidad de enfrentarnos al fraude publicitario sin rodeos, tanto para el beneficio de los consumidores a los que servimos como del sector de las comunicaciones en general.*
>
> *Es importante que trabajemos conjuntamente con nuestros colegas y socios del sector para abordar los retos a los que nos enfrentamos y que colaboremos para cambiar el funcionamiento del ecosistema actual".*

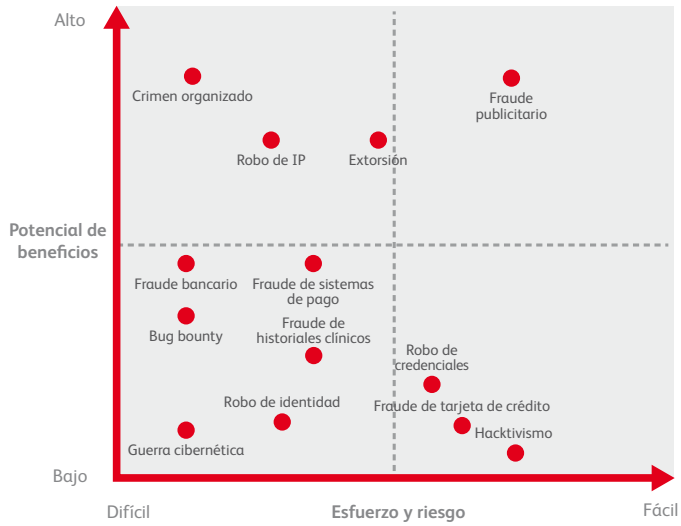
Luis Di Como,
Vicepresidente Senior de Medios Globales de Unilever y miembro del Global Transparency Group y del comité ejecutivo de la WFA

1 *Digital Content Next y White Ops > https://digitalcontentnext.org/wp-content/uploads/2015/09/DCN-Bot-Benchmark-Report-2015-.pdf*
2 *Encuesta exclusiva para miembros, noviembre de 2015 > http://www.wfanet.org/en/knowledge/global-knowledge-base#/item/314*
3 *ANA y WhiteOps. The Bot Baseline 2015 > http://www.ana.net/content/show/id/botfraud-2016*
4 *Oxford BioChronometrics > https://oxford-biochron.com/over-88-of-digital-ad-clicks-deemed-fraudulent-new-study-by-oxford-biochronometrics-suggests/*
5 *Distil Networks 2015 > http://resources.distilnetworks.com/h/i/155404518-distil-networks-releases-new-data-on-the-state-of-digital-advertising-fraud*
6 *ANA y White Ops 2014 'The Bot Baseline' > http://www.whiteops.com/botfraud*
7 *Incapsula, informe del tráfico de bots de 2013 > https://www.incapsula.com/blog/bot-traffic-report-2013.html*
8 *Incapsula, estudio sobre el fraude en aplicaciones móviles de 2015 > http://www.prnewswire.com/news-releases/forensiq-projects-in-app-ad-fraud-will-surpass-1-billion-in-2015-300117453.html*
9 *Solve Media 2014 > http://www.businessinsider.in/Botnets-Will-Cause-11-6-Billion-In-Wasted-Ad-Spending-This-Year/articleshow/29508619.cms*
10 *Trademob 2012 > https://gigaom.com/2012/08/31/report-40-percent-of-mobile-clicks-are-fraud-or-accidents/*
11 *Solve Media 2013 > http://www.adweek.com/news/advertising-branding/bot-problem-keeps-getting-worse-154585*
12 *Bin Liu, Universidad del Sur de California 2014 > https://www.usenix.org/node/179764*
13 *Deloitte y Advertising Association (Reino Unido) 2011 > http://www.adassoc.org.uk/publications/advertising-pays/*

¿QUÉ NOS DEPARA EL FUTURO?

La digitalización, los delitos informáticos y las tendencias para contrarrestar el fraude publicitario son los factores principales que determinarán el crecimiento del fraude publicitario en los próximos 10 años. A menos que la capacidad de contrarrestar el fraude publicitario aumente de forma paralela al dinero que se invierte en medios digitales, los índices de exposición al fraude publicitario aumentarán significativamente en términos absolutos.

Solo hay unos pocos casos en los que el fraude publicitario haya conllevado una acusación[14] y una condena[14], lo que significa que el nivel de riesgo es bajo en comparación con otros delitos digitales. Un informe reciente de Hewlett Packard clasifica el fraude publicitario con un 'potencial de beneficio' mayor que cualquier otro tipo de delito digital[15]. Se prevé que la combinación de estos factores atraiga a los '*spammers*', a las organizaciones de crimen organizado y a otros delincuentes que se hayan centrado en otras áreas hasta ahora.



Fuente: Hewlett Packard Enterprises, 'The Business of Hacking', Mayo de 2016

Cuanto más tiempo permitamos que crezca el fraude publicitario, más difícil será contrarrestarlo.

Se estima que en 2025 la inversión global total en medios digitales se situará en un rango de 400 000 a 500 000 millones de dólares[16]. Solo con que un 10 % del límite superior de este rango esté expuesto al fraude publicitario, este se convertiría en la segunda forma de crimen organizado[17] más rentable, solo por detrás del mercado de cocaína y opiáceos.

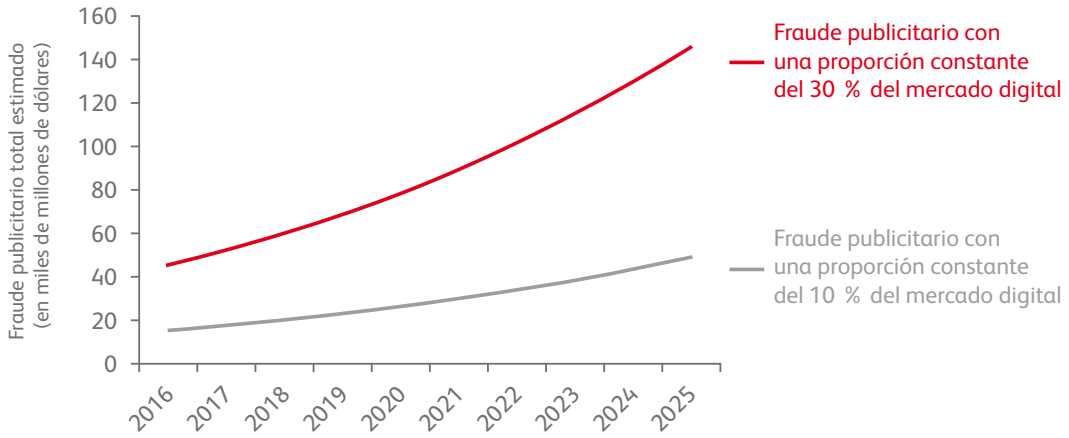
Sin embargo, como se ha mencionado anteriormente, hay estudios que identifican que el fraude publicitario representa mucho más del 10 % del mercado digital. De hecho, ya podría ser más del 30 % según el escenario más grave al que nos referimos a lo largo de este documento.

Un simple cálculo matemático determina que el 30 % de un mercado de 150 000 millones de dólares en 2016 equivale a 45 000 millones de dólares. Si asumimos que esta tendencia se mantendrá constante en los próximos 9 años, de forma que el crecimiento solo provenga de la ampliación del mercado de la publicidad digital, el fraude publicitario representaría 140 000 millones de dólares en 2025.

[14] *En concreto, cuando el FBI expuso el fraude cometido por responsables de marketing afiliados (http://uk.businessinsider.com/ebay-the-fbi-shawn-hogan-and-brian-dunning-2013-4?r=US&IR=T) y el caso en el que un individuo fue condenado en EE. UU. por un fraude de clics (http://www.reuters.com/article/us-usa-cybersecurity-malware- idUSKCN0XN2WX)*
[15] *Hewlett Packard Enterprises, 'The Business of Hacking', Mayo de 2016*
[16] *Según tendencias históricas de GroupM y ZenithOptimedia, además de previsiones de la WFA basadas en las fuerzas de mercado futuras.*
[17] *https://www.unodc.org/toc/en/crimes/organized-crime.html*

Por supuesto, es muy improbable que el fraude publicitario no crezca más allá de su base actual. Lo más probable, en realidad, será que aumente rápidamente, a medida que sus autores crezcan en sofisticación. Aunque se pueda debatir si el índice de exposición correcto es el 10 %, el 30 % o superior, difícilmente se puede negar que las previsiones que se muestran a continuación son muy conservadoras.

A menos que se produzcan cambios drásticos en el ecosistema de la tecnología publicitaria y en la forma en que los anunciantes y sus socios del sector invierten el dinero en los medios, la cifra más baja de 50 000 millones de dólares en 2025 que indica el diagrama siguiente podría parecer en poco tiempo una cifra increíblemente baja, más que una previsión conservadora.



Fuente: Previsiones del sector basadas en el crecimiento del mercado de medios digitales y posibles escenarios de crecimiento del fraude publicitario

Las investigaciones de la WFA han descubierto que 9 de cada 10 anunciantes encuestados (el 92 %) está de acuerdo en que la estructura del ecosistema de los medios digitales contribuye a perpetuar el fraude publicitario. El ecosistema, incluidos los editores y otros agentes del lado de la oferta, así como las empresas de tecnología, las agencias y otros actores del lado de la demanda, tienen el deber de demostrar que disponen de la capacidad de enfrentarse al fraude publicitario de manera eficaz. **Hasta que llegue ese momento, los anunciantes deberían ser cautos en relación con sus inversiones en medios digitales para limitar el crecimiento del fraude publicitario y su exposición al mismo.**

"El aumento de la inversión en medios digitales ofrece tantas oportunidades como retos, pero pocos son tan acuciantes como este. Debemos implantar las medidas adecuadas para proteger nuestras marcas y a nuestros consumidores. Hay mucho que aprender del sector financiero, que continúa lidiando una batalla similar contra el fraude online".

Mark Butterfield,
Director de Medios Globales, Boehringer Ingelheim Ltd y miembro del Global Transparency Group de la WFA

¿QUÉ FORMAS ADQUIERE EL FRAUDE PUBLICITARIO?

Hay tres formas básicas de fraude publicitario:

1. Sitios web. Se puede dividir en los sitios web que están directamente controlados por el infractor[19], y aquellos para los que el infractor actúa como afiliado, que es el caso típico en los fraudes de conversión.

2. Plataformas. Puede ser desde un sitio web de redes sociales hasta un sitio web de alojamiento de vídeos. Cuando las marcas están más familiarizadas con las plataformas, es inevitable que haya más confianza y menos sospecha de fraude. Hay indicios de que las principales plataformas tienen graves problemas con el fraude publicitario[20].

3. Datos. Esta categoría hace referencia a cualquier circunstancia en la que los infractores puedan monetizar los datos de los usuarios a través de mercados de datos. Se puede llevar a cabo de varias formas, pero un ejemplo sería enviar una red de *bots* para visitar sitios de editores, haciendo que estos *bots* se conviertan en parte de lo que el editor consideraría datos internos. Muchos editores utilizan *cookies* para segmentar audiencias y vender anuncios en sitios externos por medio de técnicas de extensión de audiencia, propagando de este modo las impresiones falsas en la web. Otros pasos incluyen enviar *bots* para que visiten sitios que son propiedad del anunciante, hacer pasar *cookies* como datos propios de un anunciante e infectar los datos de marca[21].

Prácticamente cualquier compra programática está expuesta al fraude publicitario; incluso las compras programáticas directas de televisión son vulnerables. Se debería desconfiar de cualquier declaración en la que se afirme lo contrario.

En el caso del fraude en sitios web, la forma más antigua y común de fraude publicitario, hay tres aspectos que cabe tener en cuenta.

1. Sitios de *spam*. Se trata de un fenómeno (explicado con más detalle más adelante) asociado especialmente al fraude publicitario. A pesar de que existe una gran cantidad de recursos para analizar e incluir en una lista negra las direcciones IP asociadas con el tráfico fraudulento, no hay ningún recurso similar disponible para los sitios de *spam* relacionados con el fraude publicitario. De los primeros 5000 sitios, según el tráfico, disponibles para los compradores de medios a través de los *ad exchanges*, casi el 30 % utiliza soluciones de privacidad, lo que hace muy difícil o prácticamente imposible conectar el sitio web con ningún individuo o empresa.

   Estos sitios web suelen enviar a los intercambios de anuncios de 10 a 100 veces más tráfico que lo que sitios como Alexa[22] consideran posible. Es muy común que un sitio así envíe cien millones de impresiones (o más) para vender en *ad exchanges* en un solo día.

2. Tráfico. Es importante entender que hay dos tipos de tráfico: uno con el que es posible la eficacia publicitaria y otro con el que no. Los ejemplos de tipos de tráfico que pertenecen a la segunda categoría incluyen:

   - tráfico de actualización automática: cuando el navegador del usuario actualiza constantemente la página (o los anuncios en la página)
   - tráfico de *clickjacking*: cuando se engaña a los usuarios para que hagan clic en algo que ellos piensan que tiene otra función[23]
   - tráfico de *cloudbot*: tráfico que proviene de direcciones IP en la nube de la empresa de alojamiento de páginas web[24]
   - tráfico normal de *botnets*: el tráfico procedente de los dispositivos de usuario infectados
   - tráfico de *cookie stuffing*: redireccionar a un usuario a un sitio web para colocarle una *cookie* afiliada en el navegador[25]
   - tráfico de granjas de clics (*farm traffic*): acciones del usuario (por lo general conversiones), repetidas por un gran número de personas[26]
   - anuncios ocultos: anuncios 'apilados' unos encima de otros o de alguna otra forma invisibles para el usuario
   - tráfico de *spam* social: enlaces engañosos publicados en las redes sociales que producen visitas inútiles

3. *Spambots*. Un *bot* social típico puede publicar contenido de varios sitios miles de veces al día. Estos *spambots* sociales se utilizan para crear la impresión de un sitio popular, ya que aparentan altos niveles de contenido compartido relacionado con el sitio.

Al final, lo importante no es si el tráfico ilegítimo está compuesto por tráfico de *botnets*, por una de las otras formas de tráfico mencionadas o por otros medios. Lo que importa es que no ofrece ninguna posibilidad de eficacia publicitaria.

La industria debe concentrarse en los dos ámbitos en los que se genera el dinero del fraude publicitario: los sitios de *spam* y la compra de tráfico.

[19] *Digiday/Mike Nolet > http://digiday.com/platforms/one-fraud-site-netted-161-million-impressions-one-week/*
[20] *http://www.ft.com/cms/s/0/53ac3fd0-604e-11e5-a28b-50226830d644.html#axzz49fKzb39V*
[21] *https://medium.com/ad-fraud/direct-buy-poisoning-how-data-fraud-leaves-transactions-vulnerable-to-fraud-a5cc25f11319*
[22] *http://alexa.com*
[23] *https://en.wikipedia.org/wiki/Clickjacking*
[24] *http://www.darkreading.com/cloudbot-a-free-malwareless-alternative-to-traditional-botnets/d/d-id/1297878*
[25] *https://en.wikipedia.org/wiki/Cookie_stuffing*
[26] *https://en.wikipedia.org/wiki/Click_farm*

SITIOS DE SPAM VIRAL Y TRÁFICO COMPRADO

La gran mayoría de los 5000 sitios principales (por inventario) disponibles en los *ad exchanges* son algún tipo de sitio de noticias virales[27]. Estos sitios, y muchísimos más como ellos, se llevan un porcentaje importante de la inversión total en medios programáticos, mientras que la calidad de su tráfico sugiere que hay muy poco margen para la eficacia publicitaria a partir de la inversión realizada.

Las características típicas de un sitio de este tipo incluyen:

Como estos sitios compiten directamente con los editores premium por el porcentaje de presupuestos globales de inversión en los medios, los editores premium se ven obligados a comprar tráfico. Algunos investigadores consideran que la compra de tráfico es una práctica muy extendida, incluso entre los editores más reconocidos.

El tráfico comprado supone para la edición de Internet lo que las sustancias para mejorar el rendimiento han sido para el deporte; si se quiere competir al más alto nivel, la forma más segura de conseguirlo es recurrir al dopaje. De forma similar al dopaje en el deporte, el tráfico comprado proporciona al editor una ventaja injusta sobre los que no lo utilizan.

El problema es que una vez se empieza con el dopaje, es casi imposible dejarlo sin que ello afecte negativamente al rendimiento.

"Aunque establecer de forma concluyente un índice creíble de exposición al fraude publicitario global o incluso local sigue siendo difícil por el momento, durante la supervisión regular de campañas para los anunciantes que son nuestros clientes principales, hemos visto muchos editores individuales con un 100 % de actividad no humana y algunos editores (premium) importantes con más de un 70 % de tráfico no humano. Aunque puede que algunos editores compren tráfico directamente a través de botnets, el tráfico no humano en los editores premium se debe principalmente al tráfico comprado de baja calidad, a las arañas web y a los scrapers".

Ehsan Mokhtari,
Presidente y Fundador de Sentrant Security y miembro del Advertising Fraud Council

El tráfico se puede adquirir de forma que cumpla los requisitos de los principales proveedores de verificación, incluidas las empresas de medición de audiencia y las empresas que luchan contra el fraude publicitario, a un precio inferior a 0,01 $ por clic. También se puede manipular para que dé la impresión de tener tasas de visibilidad superiores a las del tráfico legítimo. Mientras que los editores legítimos solo pueden ofrecer lo que realmente poseen, los autores del fraude publicitario pueden ajustar su inventario de forma que parezca más deseable para los algoritmos de compra, estableciendo una ventaja sobre los vendedores legítimos a la hora de ganar las pujas de los compradores.

Los anunciantes pueden encontrar recomendaciones sobre cómo gestionar mejor y limitar su exposición al tráfico comprado en el reciente informe de la ANA (Asociación Nacional de Anunciantes estadounidense): "Sourced Traffic: Buyer Beware". Las recomendaciones incluyen exigir transparencia e informes de las agencias, establecer objetivos de campaña razonables y prestar atención a los editores "mid-tail" y "long-tail".

El informe también hace referencia a los Publisher Sourcing Disclosure Requirements (PSDR), un conjunto de directrices desarrolladas por el Trustworthy Accountability Group (véase la pág. 18 que se encuentra a continuación), en el cual se exige a los editores que revelen el porcentaje que representa el tráfico comprado en la totalidad de su recuento de audiencia

Los algoritmos también pueden dar prioridad a ciertos sitios de *spam* viral frente a otros, debido a la percepción de que ofrecen un inventario más 'apetecible'. Esto está relacionado con el uso extendido de la segmentación *run-of-exchange* por parte de los *trading desks* y las plataformas de demanda, un hecho que se puede comprobar fácilmente investigando los registros de compra específicos para un anunciante de cualquier DSP. Uno de los factores más atractivos para un editor es su capacidad de satisfacer cualquier volumen de demanda. Debido a la presión a la que están sometidos los *trading desks* para satisfacer los objetivos presupuestarios, que los clientes suelen priorizar frente a otros criterios de demanda, se puede influir sobre los algoritmos de las plataformas de compra para que compren sitios de baja calidad[28].

Mientras no se sustituyan las compras *run-of-exchange* por una forma más adecuada de alcanzar los mismos objetivos, los sitios de spam seguirán acaparando gran parte del mercado de la publicidad programática, que ya representa más de 200 000 millones de eventos al día.

[27] *Botlab.io Media 5k > http://botlab.io/media5k/*
[28] *http://www.minonline.com/news/The-Bots-Have-It-Ad-Fraud-and-Premium-Pubs_26247.html#.VzRM3hUrK7p*

¿QUIÉN COMETE EL FRAUDE PUBLICITARIO?

Los autores principales del fraude publicitario son los llamados profesionales del marketing 'de sombrero negro', expertos en tecnología de marketing. Otros infractores incluyen las redes publicitarias ilegítimas y los delincuentes informáticos.

Por ahora, la implicación del crimen organizado en este ámbito es limitada, pero es muy probable que esto cambie a medida que los delincuentes que se han dedicado tradicionalmente al *spam* y a otros delitos informáticos se vayan introduciendo en el fraude publicitario. Para detener ese progreso se necesitan precedentes legales de sentencias comparables con las de otros delitos informáticos en las jurisdicciones principales. Ese es uno de los factores clave para evitar lo que de otra forma podría suponer un incremento drástico del fraude publicitario.

El fraude publicitario suele estar perpetrado por los siguientes infractores que se dividen en tres grupos diferenciados, cada uno con niveles distintos de habilidad y de dedicación a esta práctica.

	HABILIDAD	DEDICACIÓN	AMENAZA
Infractores del mundo del marketing			
Profesionales del marketing de sombrero negro	EXPERTO	MUY ALTO	MODERADO
Ciertas redes publicitarias ilegítimas	MODERADO	BAJO	MODERADO
Infractores criminales			
Delincuentes informáticos comunes	MODERADO	BAJO	BAJO
Crimen organizado	MODERADO	ALTO	ALTO

Fuente: categorías y descriptores basados en la investigación y la experiencia del Advertising Fraud Council. Amenaza se refiere al nivel de amenaza que supone esa clase de infractor para la sociedad.

Profesionales del marketing de sombrero negro. Muchos profesionales del marketing de sombrero negro tienen experiencia previa en administración de sitios web, marketing de afiliados o SEO avanzado. Aunque operan en solitario, son capaces de hacerlo a gran escala y suelen ser expertos en tecnología de marketing, con amplios conocimientos sobre persuasión y psicología inversa.

Ciertas redes publicitarias ilegítimas. Existen redes o plataformas publicitarias que participan conscientemente en el fraude publicitario, actuando a menudo como intermediarias entre los profesionales de marketing de sombrero negro y los intercambios de publicidad. Entre estas redes publicitarias son habituales los modelos de rendimiento (CPA). Algunas de estas redes publicitarias parecen totalmente legítimas durante una inspección superficial y a menudo obtienen dólares de publicidad premium directamente de las marcas o de sus agencias colaboradoras.

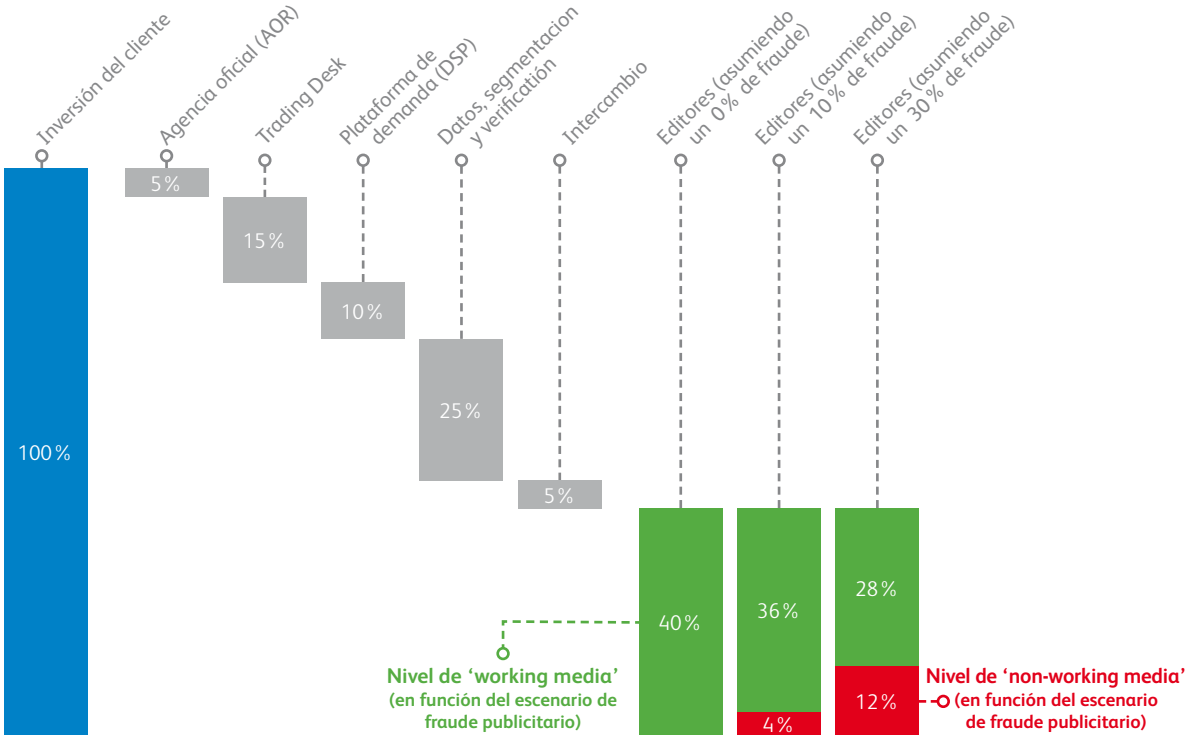
Delincuentes informáticos comunes. Con antecedentes de delitos informáticos, *spam* y *phishing*, por ejemplo, los delincuentes informáticos pueden verse atraídos por el fraude publicitario por el gran potencial de beneficios que ofrece.

Crimen organizado. Es probable que otro tipo de delincuentes sin antecedentes en delitos informáticos también se vayan introduciendo en este ámbito. El modelo de crecimiento presentado en este informe predice que, de continuar la trayectoria actual, el fraude publicitario será el segundo delito más rentable en 2025, superado únicamente por el mercado de cocaína y opiáceos.

EL FLUJO DE DINERO DEL FRAUDE PUBLICITARIO:
CÁLCULO DEL COSTE EN TODA LA CADENA

Los anunciantes pueden comprar medios digitales de varias formas, pero la compra programática es, con diferencia, el medio que presenta un mayor crecimiento. Entre las muchas razones que lo explican, destaca el hecho de que muchos anunciantes han identificado una serie de mejoras en el rendimiento como resultado de la compra programática. Sin embargo, esta infraestructura compleja ha servido para empeorar las vulnerabilidades del ecosistema, como señala el documento WFA's guide to Programmatic Media Management (Informe de la WFA sobre compra programática) [29].

Dado que se prevé que la compra programática se convierta en el método universal para todo tipo de medios, hemos tomado una compra programática típica como base para el siguiente análisis. Aquí se ilustra dónde interviene el fraude publicitario en el ecosistema y el efecto que causa en la inversión de un anunciante a lo largo del proceso.



Fuente: previsiones del sector

En una compra programática típica intervienen varios intermediarios, entre los que se incluyen *trading desks*, plataformas de demanda (DSP), proveedores de verificación, etc., cada uno de los cuales exige una parte de la inversión del anunciante.

Aproximadamente el 40 % del gasto lo reciben los editores que tienen acceso a los usuarios al final de la cadena. Los llamados '*working media*'. Pero la realidad es que parte del tráfico es fraudulento y no ofrece posibilidades de eficacia publicitaria.

Tras introducir los escenarios de exposición al fraude publicitario establecidos anteriormente en este documento, los niveles de *working media* van decayendo inevitablemente: un 36 % si se aplica el nivel de exposición del 10 % y solo un 28 % de *working media* en el escenario del 30 % de fraude publicitario.

[29] *WFA Guide to Programmatic Media 2014 (Informe de la WFA sobre compra programática 2014) > www.wfanet.org/programmatic*

Antes de que el autor del fraude entre en la cadena, la industria 'formal' ya se ha visto implicada y ha recibido el pago por su parte en el proceso. Naturalmente, esto es así sea cual sea el nivel de exposición al fraude publicitario e independientemente de si la red publicitaria o el editor son legítimos o participan en el fraude publicitario.

En los dos escenarios de exposición considerados en este análisis, **el principal beneficiario del fraude publicitario (aunque no deliberadamente) es la industria del marketing. Mientras que en el escenario del 30 %, el 12 % de los ingresos procedentes del fraude publicitario lo obtienen sus autores, el 18 % restante lo absorbe el ecosistema legítimo.**

No es acertado suponer que al negociar directamente con los editores (programático directo) se elimina todo el riesgo de exposición al fraude. Los sitios de *spam* que aparentan ser premium imperan en los intercambios, e incluso algunos editores premium legítimos presentan riesgos de fraude publicitario debido al uso del tráfico comprado (mencionado anteriormente), junto a otros factores.

Debido a los ingresos que obtienen del ecosistema de medios digitales, la mayoría de las empresas de tecnología publicitaria y plataformas de publicidad carecen de motivación para tomar las acciones urgentes que se necesitan para crear un ecosistema seguro y transparente en la publicidad online. **Como resultado, los costes del fraude publicitario recaen exclusivamente en los anunciantes y los contribuyentes.** Los anunciantes no obtienen ningún margen de efectividad por su inversión, y en algunos casos los ordenadores de los consumidores pueden resultar infectados por *malware* para llevar a cabo acciones fraudulentas, aparentemente por parte del propio usuario.

EL FLUJO DE DINERO DEL FRAUDE PUBLICITARIO:
CÓMO TIENEN LUGAR LAS TRANSACCIONES

La persistencia del problema del fraude publicitario está estrechamente relacionada con las políticas y prácticas que emplean otras partes implicadas a la hora de pagar a los editores con los que colaboran. En muchos casos, una red publicitaria o *ad exchange* importante solo cuenta con una dirección de correo electrónico para ponerse en contacto con un editor al que están pagando decenas o cientos de miles de dólares al mes. Puede que nunca hayan conocido en persona a ningún individuo asociado con ese editor. Y a pesar de ello, es probable que se acaben realizando transacciones de millones de dólares entre ambas partes de esta forma. Cuanto más grande sea la red publicitaria, más difícil resulta ser diligente al respecto.

Transacciones del fraude publicitario, cuando las compras programáticas se realizan a través de un *trading desk*

1. El anunciante paga a la agencia.
2. La agencia paga a la plataforma de demanda.
3. La plataforma de demanda paga al intercambio.
4. El intercambio paga al editor (o a una red publicitaria intermediaria que a su vez paga al editor).

Todas las transacciones tienen lugar a través del sistema bancario oficial, conforme a las prácticas de contabilidad de las grandes empresas. **De esta forma el editor, que de hecho podría ser un delincuente informático a gran escala, puede operar como parte de la economía formal.**

Las empresas ficticias son habituales para desvincular aun más al infractor de la actividad fraudulenta en la que está implicado. Estas empresas se pueden establecer rápidamente y a gran escala. Por lo general, las redes y plataformas publicitarias no examinan lo suficiente a sus colaboradores, a los que a menudo ni siquiera llegan a conocer en persona, por lo que es tan sencillo como operar bajo una identidad falsa, como por ejemplo una identidad adquirida en el mercado negro.

En definitiva, cuanto más grande sea la red o plataforma publicitaria legítima, mayor será su cuota en la economía total del fraude, aun cuando no esté implicada en dicha actividad ni tenga ninguna intención de obtener ingresos procedentes del fraude publicitario.

GUÍA DEL ANUNCIANTE PARA CONTRARRESTAR EL FRAUDE PUBLICITARIO

El fraude publicitario es complejo, como también lo son los diversos aspectos que lo componen y lo causan, pero un anunciante individual puede lograr un gran avance en términos de resultados a corto plazo. **Sin embargo, a menos que haya una reacción de los principales anunciantes acompañada de un enfoque común para afrontar el problema, incluso los beneficios individuales a corto plazo disminuirán rápidamente mientras los problemas estructurales subyacentes del sector de la publicidad continúen creciendo en magnitud y complejidad.**

Esta guía no pretende hacer un resumen de los diversos métodos de investigación y análisis de datos contra el fraude publicitario, de los métodos de detección o de la información que se encuentra fácilmente disponible en el contexto del fraude publicitario. En un mercado del fraude publicitario que se mueve rápidamente, utilizar esos métodos en solitario sin los consejos que se indican a continuación conllevará, en el mejor de los casos, obtener ingresos individuales a corto plazo, y en el peor, que los infractores desarrollen un mayor grado de sofisticación.

La única forma de cambiar las cosas es conseguir un cambio de conducta eficaz. En este caso, comprender, gestionar y contrarrestar de forma satisfactoria el fraude publicitario. El cambio **de conducta** es el resultado de unos **desencadenantes** que nos recuerdan por qué es importante cambiar una conducta determinada; unas **motivaciones** que enfatizan la seriedad del cambio necesario, y unas **capacidades** que permiten que el cambio se produzca.

1. PERSONAS Y TECNOLOGÍA

Desarrolle recursos internos.

Puesto que todas las soluciones de terceros las proporcionan pequeñas *startups* o empresas que previamente se han estado dedicando a otros ámbitos, **es fundamental contar con expertos internos que avalen la selección de proveedores y otras decisiones, aunque solo sea una persona la que se encargue de estas tareas.** Por ahora, no se recomienda confiar en exceso en los proveedores de verificación de terceros. Ni tampoco confiar en que su agencia se encargará de contrarrestar el fraude publicitario, ya que las agencias aún no están incentivadas ni equipadas para ello.

Anime a los proveedores de terceros a utilizar soluciones abiertas.

Una de las claves del éxito, tanto con los sistemas de detección de intrusiones como con el filtrado de spam en correos electrónicos (dos ámbitos destacados de la lucha contra delitos informáticos similares al fraude publicitario), es que incluso los proveedores más importantes y respetados en la actualidad utilizan las mismas soluciones abiertas como base para su oferta privada. El éxito conseguido en la seguridad de la red (detección de intrusiones) y en la detección de correo no deseado mediante el uso de tecnologías comunes y abiertas ilustra la necesidad de adoptar el mismo enfoque con el fraude publicitario, en contraposición con las soluciones tácticas privadas. **Las soluciones puramente privadas se reducen fácilmente a un juego del gato y el ratón con el infractor en el mejor de los casos, y en el peor contribuyen a mejorar sus habilidades.** Cuando se implementan soluciones privadas de terceros contra el fraude publicitario, se recomienda realizar pruebas aleatorias frecuentes comparándolas con otras soluciones para supervisar la fidelidad de la tecnología.

Colabore estrechamente con expertos en seguridad informática.

La mayoría de los principales anunciantes ya colaboran en gran medida con empresas de seguridad informática. Estas empresas cuentan con una trayectoria establecida de reducción sistemática de la exposición a problemas similares al fraude publicitario y, además, estarán menos predispuestas a favor de un método concreto contra el fraude publicitario. Colaborar con empresas del ámbito de la seguridad informática externas a la tecnología publicitaria es una forma sencilla de mejorar nuestro conocimiento de las amenazas habituales relacionadas con la publicidad en Internet y de obtener una evaluación objetiva de los proveedores de tecnología publicitaria y sus soluciones.

Exija transparencia total para su inversión.

Gran parte de la inversión en medios actual es hasta cierto punto opaca en lo que respecta al intercambio. **La transparencia debe empezar con una declaración completa y precisa de los sitios de referencia (sitios web) relacionados con inversiones por encima de cierto nivel de inventario.** La forma en la que las agencias de medios informan de las inversiones es otra causa habitual de que los anunciantes no conozcan toda la información sobre cómo se utiliza su dinero. Insistir en la transparencia a este nivel a lo largo de todo el ecosistema es una de las formas más rápidas y eficaces de sentar las bases para un entorno comercial más seguro.

2. INFORMACIÓN Y COMUNICACIÓN

Establezca expectativas claras.

Al revisar los incentivos de los colaboradores y de los contratos se debe empezar por exponer claramente las expectativas. Por ejemplo, decir que no puede haber ningún fraude no es una expectativa razonable, ya que esto obligará al colaborador a encontrar maneras de informar de algo que simplemente no es posible. Es de vital importancia asimilar que es muy probable que siga existiendo un porcentaje de exposición al fraude publicitario de hasta el 10 %, por muchas medidas que se tomen. Desconfíe de cualquier proveedor que asegure lo contrario.

Establezca los indicadores adecuados.

Los colaboradores no están lo suficientemente incentivados como para evitar el fraude; un problema que se sitúa en la raíz de la epidemia. Hay que ser conscientes de que pasar de CPM a CPC o CPA no es la solución para reducir el fraude publicitario: en la mayoría de los casos empeorará el problema y lo hará más difícil de resolver. La única excepción son aquellos casos en los que los pagos por acuerdos de CPA se basan en los resultados de negocio reales, como un cliente nuevo para un banco o artículos vendidos que ya no son reembolsables. A modo de ejemplo, un banco no obtiene ningún valor de negocio de una aplicación de tarjeta de crédito obtenida a partir de un acuerdo de CPA, pero sí de un cliente que realiza un depósito en una cuenta bancaria o que utiliza la tarjeta del banco en cuestión. En la medida de lo posible, los indicadores de desempeño deben reflejar los resultados de negocio del anunciante.

Comparta información abiertamente.

Los hallazgos relacionados con el fraude publicitario deberían compartirse con todos los colegas posibles, tanto internos como externos, y con tanto detalle como sea legalmente posible. Es fácil desplazar el fraude publicitario pero muy difícil reducirlo, por lo que compartir información abiertamente entre todos es la clave del éxito para todas las partes implicadas. Colaborar y compartir la información abiertamente es uno de los ámbitos en los que la industria formal puede hacerlo mejor que los infractores, que suelen operar totalmente aislados unos de otros o incluso mostrar hostilidad entre ellos.

"Puede que sea imposible conseguir un inventario de publicidad completamente libre de fraude. Sin embargo, debemos mantenernos firmes. Colaborando juntos, compartiendo conocimientos interna y externamente, y estableciendo objetivos en los que podamos progresar, poco a poco. Nosotros estamos aplicando este mismo enfoque a la visibilidad y está funcionando".

Gerhard Louw,
Medios Internacionales de Deutsche Telekom AG y miembro del Global Transparency Group de la WFA

3. NORMAS

Listas que sustituyan las compras *run-of-exchange*.

Las compras *run-of-exchange* (ROE) se deberían evitar. Estas compras, en las que se adquieren anuncios a ciegas por millones de sitios, son una forma segura de aportar dinero al fraude publicitario. Las compras ROE benefician a los proveedores de tecnología publicitaria y carecen de otros beneficios en sí mismas. Un típico argumento en contra por parte de los proveedores es que este es el único modo de que una plataforma publicitaria pueda cumplir los objetivos presupuestarios en términos de gasto total por campaña o a lo largo de un periodo de tiempo determinado. Un argumento que por sí mismo indica claramente los graves problemas estructurales del sector. A corto plazo, los anunciantes tienen que aceptar que, en algunos casos, los "objetivos" de la inversión en medios digitales no se podrán alcanzar sin exponer las compras a altos niveles de fraude.

Una base de datos de sitios web comunes.

Una base de datos de sitios web mantenida por una entidad independiente, en la que los indicadores de calidad y otros factores clave para la transparencia estén disponibles de forma gratuita y abierta para todo el ecosistema. Si la inversión en un sitio web supera cierto importe en un periodo determinado, se debería exigir a ese sitio web que incluya información adicional sobre su negocio en la base de datos común.

Una base de datos de proveedores de tecnología publicitaria.

Salvo en las plataformas publicitarias más conocidas, puede ser muy difícil averiguar qué empresa está detrás de una etiqueta publicitaria. Las etiquetas que manejan una gran cantidad de solicitudes suelen estar alojadas en dominios que solo tienen semanas o meses de antigüedad y utilizan un nombre de dominio desconocido combinado con una protección total de la privacidad. Aunque un investigador quisiera obtener una idea del flujo de tráfico del anuncio y del flujo de dinero resultante, esto solo sería posible a un nivel relativamente superficial. Para solucionar este problema de manera eficaz, es necesaria una base de datos de proveedores comunes. Este es un ejemplo donde iniciativas como el Trustworthy Accountability Group (TAG*) estadounidense podrían ser de utilidad.

**TAG es un programa de contabilidad entre varios sectores. Este programa conjunto de los sectores del marketing y de medios se creó en torno a cuatro áreas principales: el tráfico fraudulento de publicidad digital, combatir el malware, la piratería de Internet financiada por anuncios y promover la seguridad de las marcas. TAG fue creado por la Asociación Nacional de Anunciantes estadounidense (ANA), la American Association of Advertising Agencies (4A's) y el Interactive Advertising Bureau (IAB), y colabora con empresas en toda la cadena de suministro de la publicidad digital.* http://www.tagtoday.net/

4. GESTIÓN

Cambios contractuales.

Se deben revisar los contratos con las agencias y proveedores de forma que la responsabilidad contractual se convierta en la principal motivación para el cambio de conducta de los colaboradores. Se debe hacer hincapié en las sanciones por asignar gastos a inventarios relacionados con el fraude publicitario, en aquellos casos en los que se pudiera haber evitado.

Colaboración con las autoridades.

Los anunciantes pueden ayudar compartiendo hallazgos y datos e informando a las autoridades pertinentes de problemas importantes en el ecosistema. La Incorporated Society of British Advertisers (ISBA) del Reino Unido se ha embarcado en una iniciativa como esta* junto con la policía de Londres en relación con la seguridad de las marcas.

**La ISBA ha trabajado codo con codo con la unidad de delitos contra la propiedad intelectual de la Policía de Londres como parte de una colaboración única entre la policía y el sector de la publicidad digital del Reino Unido para luchar contra las actividades ilegales relacionadas con la publicidad online. Su objetivo es proteger a los anunciantes asegurándose de que sus anuncios no aparezcan en sitios web ilegales que infrinjan direcciones de IP, privando así a estos sitios web de los ingresos que los anunciantes les proporcionan involuntariamente.*

Ejercer presión para conseguir repercusiones legales equivalentes a las de otros delitos similares.

Como no hay un precedente legal de sentencias, las autoridades competentes no cuentan con los recursos apropiados para investigar seriamente los delitos de fraude publicitario, independientemente de la magnitud de la operación o de otros factores.

Exigir a los colaboradores compensaciones retroactivas.

Las comisiones o tasas obtenidas por las redes, plataformas o agencias publicitarias en campañas sujetas al fraude publicitario se deberían devolver a sus respectivos anunciantes. Exigir compensaciones es importante porque transmitirá al ecosistema de los proveedores el mensaje de que ya no es posible obtener comisiones de la inactividad pasiva.

"No se trata de buscar a culpables, sino de empezar a encontrar soluciones factibles para los anunciantes. Se necesita un cambio de conducta por parte de todos los actores implicados en este ecosistema. No solo los propietarios de marcas, sino todos aquellos a los que confiamos nuestra inversión y especialmente nuestras agencias colaboradoras".

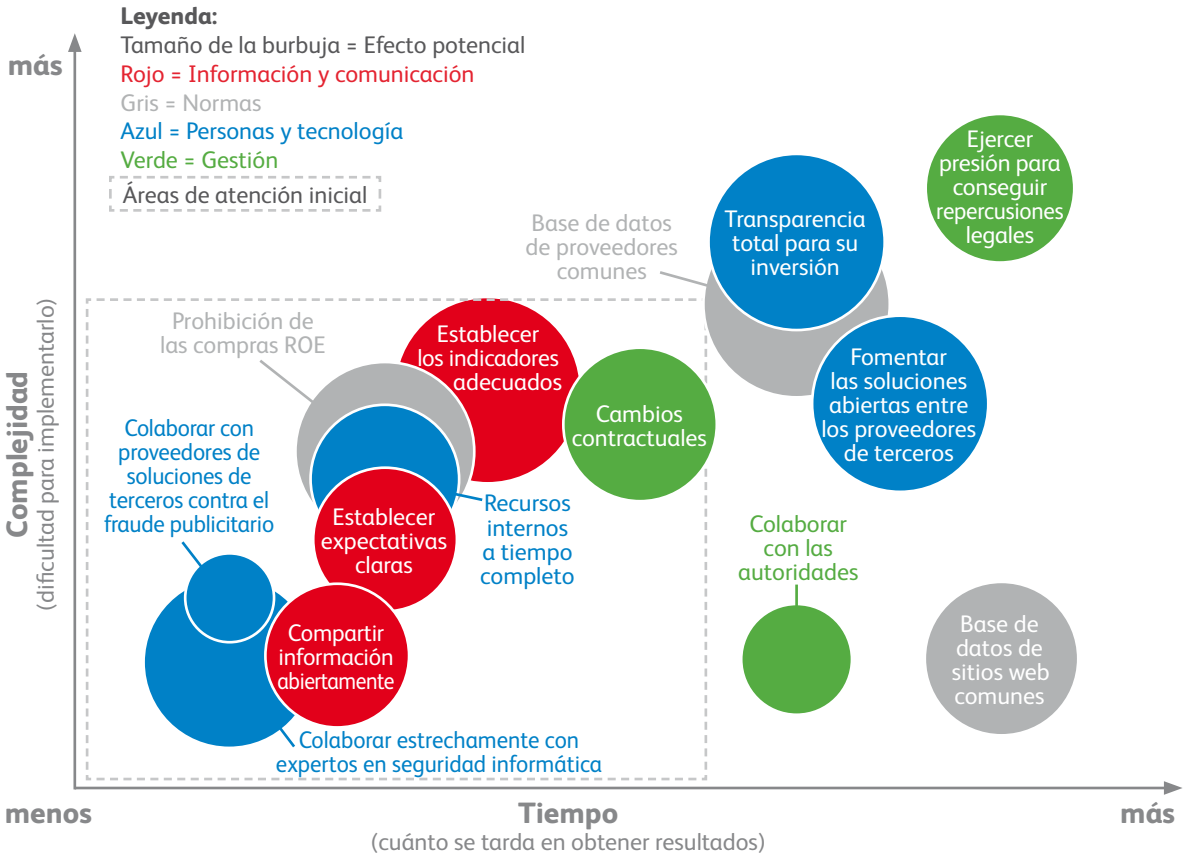
Sital Banerjee,
Jefe Global de Medios de Philips y miembro del Global Transparency Group de la WFA

¿QUÉ MEDIDAS PUEDEN ADOPTAR LOS ANUNCIANTES?

Las acciones descritas hasta ahora se pueden clasificar por tiempo (cuánto tardan en ofrecer resultados), efecto (magnitud del resultado) y complejidad (la dificultad para llevarlas a cabo).

Muchas de las soluciones mencionadas en este documento caen dentro del cuadrante inferior izquierdo del gráfico. Como son relativamente menos complejas y se necesita menos tiempo para implementarlas, las hemos recomendado como "áreas de atención inicial". Colaborar con empresas de seguridad informática y compartir la información abiertamente son acciones claras en las que centrarse en cuanto a la relativa facilidad para llevarlas a cabo, mientras que establecer los indicadores adecuados podría tener el mayor efecto en general.

Al otro lado del espectro, la presión por conseguir repercusiones legales no debería descartarse por su relativa complejidad y el tiempo que requiere implementar el proceso. Pocas señales en el mercado pueden ser tan claras como esta a la hora de transmitir las intenciones de la comunidad de anunciantes.



"El problema al que nos enfrentamos es complejo y puede parecer intimidatorio, pero ignorarlo y mirar hacia otro lado no es una opción válida. Para muchas marcas que se han pasado la última década o más defendiendo una mayor inversión en medios digitales no son buenas noticias.

La respuesta es no abandonar los medios digitales ni reprimir la innovación. Sin embargo, debemos ser mucho más prudentes y mejorar en gran medida nuestras aptitudes en esta lucha. La WFA centrará sus esfuerzos en seguir desarrollando soluciones para que nuestros miembros protejan sus marcas y sus inversiones.

Pero el resto del sector también tiene el deber de aceptar la necesidad de cambio; dejar a un lado los intereses particulares y aceptar la posibilidad de usar soluciones abiertas similares a las que han demostrado ser eficaces contra otros tipos de delitos informáticos.

No será tarea fácil. Pero estamos convencidos de que, de forma colectiva, nuestro sector puede abordar el reto para beneficiar al ecosistema digital y a la sociedad en general".

Stephan Loerke,
Director General de la WFA y miembro del Global Transparency Group de la WFA

GLOSARIO

Ad stacking (apilamiento de anuncios) > una técnica de fraude en la que se superponen varios anuncios en un único espacio publicitario de una página, lo que supone que los anuncios que quedan debajo de la capa superior no son visibles.

Extensión de audiencia > una práctica utilizada por los editores en aquellas situaciones en las que no pueden satisfacer la demanda de su inventario de publicidad. Un editor puede usar sus datos de audiencia internos para comprar la misma audiencia en otros sitios web y vender inventario como propio. Esta técnica presenta un riesgo de reducción significativa en la calidad del inventario frente al inventario propio del editor, mientras que los anunciantes pueden tener la impresión de que sus anuncios solo se ven en el sitio del editor.

Botnet > un '*bot*' es un tipo de *malware* que se utiliza para controlar un ordenador o dispositivo móvil infectado. Un grupo o red de máquinas que han sido captadas de esta forma y que controla un mismo atacante se conoce como una '*botnet*'.

Fraude de clics > cuando clics fraudulentos se hacen pasar por legítimos.

Fraude de conversión > cuando acciones de usuario fraudulentas, como suscripciones para recibir más información sobre un producto, se hacen pasar por legítimas.

Cookie stuffing > una técnica en la que se coloca una *cookie* afiliada de un sitio web de terceros en el dispositivo de un usuario sin que este haya visitado el sitio web de terceros en cuestión.

Fraude de datos > cuando los datos (propios o de terceros) se adulteran de forma que las *cookies* u otros identificadores se conectan a *bots* y no a usuarios. En otros casos, los identificadores pueden estar correctamente asociados a los usuarios, pero la información de las acciones puede ser errónea como resultado de la actividad fraudulenta.

Datos propios > SUS datos. Estos son los datos recopilados a partir de sus clientes/audiencias, que pueden incluir: comportamientos, acciones o intereses demostrados en su(s) sitio(s) web; datos personales de su base de datos de CRM; datos de suscripción, o datos sociales propios.

Granjas de fraude (fraud farms) > un enfoque llevado a cabo por humanos, en el que el fraude (normalmente un fraude de conversión) se comete a bajo coste utilizando mano de obra barata. Suele ser más habitual en países en vías de desarrollo.

Fraude de impresión > cuando impresiones fraudulentas se hacen pasar por legítimas.

Sistemas de detección de intrusiones (Intrusion Detection System, IDS) > un IDS es un dispositivo o una aplicación de software que controla las actividades de una red o sistema en busca de actividades maliciosas o infracciones de las políticas.

Run Of Exchange/s (ROE) > un tipo de segmentación habitual en el que el inventario se compra en cualquier sitio disponible a partir de los intercambios, accesible a través de una plataforma de compra publicitaria determinada.

Spambots sociales > bots que comparten enlaces de plataformas sociales.

Tráfico comprado (sourced traffic) > tráfico falso que se adquiere en el mercado de compra de tráfico. Por lo general, se origina a partir de barras de herramientas (inyecciones) y otros tipos de *adware, cloudbots, botnets* convencionales u otras fuentes fraudulentas.

Sitios de spam > sitios web que se suelen centrar en hacer de intermediarios para el tráfico comprado en el ecosistema legítimo de la publicidad online o que participan en otros tipos de actividades fraudulentas.

Datos de terceros > son los datos generados en otras plataformas y a menudo acumulados desde otros sitios web. Se pueden utilizar con fines puramente de marketing o para aumentar y mejorar los datos propios.

Web crawler (araña web) > un *bot* de Internet que rastrea sistemáticamente la *World Wide Web*, por lo general con el objetivo de indexar páginas.

Web scraper > técnica de software para extraer información de los sitios web.

Botlab.io es una fundación que se dedica a investigar el fraude publicitario, las vulneraciones de los derechos de los usuarios y otras prácticas maliciosas en la cadena de suministro de la tecnología publicitaria. Es el único grupo de defensa pública centrado en los usuarios de Internet que está fundado por antiguos miembros del sector de la tecnología publicitaria y liderado por investigadores. El director de Botlab.io es Mikko Kotila, un veterano de la publicidad en Internet con una respetada trayectoria de innovación e influencia en el sector de la tecnología publicitaria. Mikko ha estado investigado activamente el fraude publicitario y otros temas relacionados desde 2005, cuenta con más de 20 años de experiencia como investigador de Internet y trabaja en Botlab.io como voluntario a tiempo completo. Mikko es coautor de esta guía junto con la WFA.

Advertising Fraud Council es una iniciativa de colaboración en investigación y abogacía impulsada por Botlab.io que se centra en investigar a fondo el tema del fraude publicitario. El comité está formado por un líder *antifraude* de una empresa puntera de tecnología publicitaria, el director ejecutivo de una *startup* contra el fraude publicitario, un investigador de seguridad independiente, un profesor académico, un consultor independiente experto en fraude publicitario y un líder sin ánimo de lucro. Los miembros de este comité colaboran estrechamente compartiendo recursos y datos, así como a través de la investigación y el desarrollo conjuntos.

La WFA es el organismo portavoz de profesionales del marketing de todo el mundo, que representan el 90 % del gasto mundial en comunicaciones de marketing con casi 700 000 millones de dólares estadounidenses al año, con una red internacional única que incluye a los profesionales del marketing más destacados del mundo y los mayores mercados. La WFA fomenta las comunicaciones de marketing eficaces y responsables en todo el mundo. Más información en www.wfanet.org

WFA - Federación Mundial de Anunciantes
Avenue Louise 166
B-1050 Bruselas – Bélgica
+32 2 502 57 40
info@wfanet.org wfanet.org @WFAmarketers