
FRAUDE
El lado oscuro del Marketing Digital

AGRADECEMOS LA PARTICIPACIÓN A:

Didier Beauclair
Director de Estrategias y Medios
UDA

Grace Paynot
Responsable de Marketing Digital, CRM y Comunicación
PSA BANQUE

Thomas Hadjadj
Digital Acquisition Marketing Manager Head of Display Europe
MEETIC

Paulo Esteves
Head of Marketing
SELENCY

Alexandre Schont
Business Development Manager
TABMO

Fabien Omont
Data & Attribution Manager
OATH

Jeremy Giacomini
Chief Digital Officer
FONCIA

PUBLICADO: SEPTIEMBRE 2017
Trabajo realizado por miembros del Colegio de Tecnologías
de E-marketing del Colectivo para los Actores del Marketing Digital (CPA):

CORREDACTORES

Christophe Bosquet
Co-founder & CEO
effinity

Emmanuel Brunet
CEO
EULERIAN

Damien Mora
Head of Operations
Gamned!

Stéphane Gendrel
CEO & Founder
adloop

Margarita Zlatkova
Head of Performance Media & Programmatic
affilinet

Rémi Pesseguier
Partner, Head of Digital Strategy Consulting
esv digital

Philippe Baron
Data Expert
Sirdata

Noella Boullay
Delegada General

Joy Grand
Responsable de comunicación

ÍNDICE

PREFACIO

Las inversiones de los anunciantes en publicidad digital aumentan constantemente. En España, eran alrededor de 3150 millones de euros en 2019 (fuente IAB Spain), mientras que a escala mundial, esta cifra se estima en alrededor de 306000 millones de euros (fuente MAGNA).

A medida que las inversiones progresan, los caminos que toman se vuelven más complejos. Las cadenas de intermediarios se alargan, los proveedores de servicios técnicos se multiplican. La distancia entre los editores y los creadores de contenidos sigue aumentando, en detrimento del seguimiento de los importes en juego. Es legítimo que los anunciantes se preocupen por los rendimientos y el retorno de la inversión y, a este respecto, la industria de la publicidad en internet está haciendo todo lo posible para proporcionar pruebas y cuantificación de su eficacia (¡a riesgo de que los anunciantes se equivoquen en los indicadores y tomen gato por liebre!). El tamaño del mercado, la complejidad de las estructuras, la obsesión por los resultados: en este inmenso crisol global de la publicidad digital, se dan todos los ingredientes para que florezca un fraude a gran escala, que atraviesa las fronteras.

Ya un gran número de anunciantes han tomado conciencia de la necesidad de armarse contra el fraude digital, pero ¡la hidra de Lerna, con sus siete cabezas, parece poca cosa en comparación con la multiplicidad de formas que puede adoptar el fraude! En 2016, la UDA participó en la preparación del Compendio de conocimientos sobre el fraude publicitario para los inversores en medios de comunicación publicado por la WFA (Federación Mundial de Anunciantes), que elaboró un inventario inicial del fraude e incluso estimó que para 2025 podría representar entre el 10 y el 30% del total del mercado de publicidad digital. Operado por marketers sin escrúpulos, o incluso por aquellos a los que la WFA llama discretamente criminales organizados, el fraude digital va mucho más allá del mercado publicitario.

En vista de la magnitud del fenómeno y los riesgos que plantea no sólo para nuestra economía, sino también para nuestra sociedad, es esencial que todos nosotros -plataformas, anunciantes, agencias, editores...-

• Trabajemos juntos para frenar el fraude. En esta lucha común, la primera medida que se debe tomar es informar y concienciar a todo el mundo, y este es el reto de este documento. Al elaborar una lista lo más exhaustiva posible de las diferentes formas que adopta el fraude digital (¡hasta la fecha!), permite a todo el mundo estar atento a partir de ahora y establecer, siempre que sea posible, medidas de protección.
Paralelamente a su movilización contra el fraude, la UDA y sus asociados han adoptado muchas medidas para mejorar la calidad de la publicidad en internet. En particular, podemos citar lo siguiente:

• El sello Digital Ad Trust. Lanzado en Francia en el otoño de 2017 por anunciantes, agencias de medios de comunicación, agencias de internet y editores, permite que los sitios que cumplen los criterios obtengan la etiqueta DAT. Los criterios abarcan cinco áreas principales: control del fraude, calidad de la experiencia del usuario, respeto de los datos personales, visibilidad de la publicidad y protección de las marcas.

• La *Coalition for better ads*. Una iniciativa internacional, la «coalición», apoyada en particular por la WFA, ya ha publicado una lista de formatos considerados intrusivos y directamente susceptibles de promover la penetración de los bloqueadores de publicidad entre los usuarios .

• La *European viewability certification framework*. Resultado de una colaboración interprofesional europea, esta iniciativa crea el marco para una certificación de las herramientas utilizadas para medir la visibilidad de la publicidad digital.

Crear conjuntamente un mercado de la publicidad digital transparente, controlado, medido y respetuoso con el Internauta, tanto a nivel nacional como europeo y mundial, he aquí el reto de la acción de la UDA y sus colaboradores para restablecer la confianza.

Esta iniciativa de la CPA es una parte directa de ella y la acogemos con satisfacción.

Didier Beauclair
Director de Estrategias y Medios
Unión de los Anunciantes
UDA

PREFACIO

Coloquemos la primera piedra...

¡El fraude es inherente al hombre! De hecho, está presente en todas las actividades humanas. El deporte, la política, el juego, las finanzas, los negocios, etc., Dondequiera que haya reglas y ganancias potenciales, existen personas u organizaciones que tratan de esquivar estas reglas en su favor para atribuirse parte de las ganancias. Si hacer trampa no es jugar, defraudar, ¡es a menudo ganar!

Entonces, ¿es de extrañar que lo digital, un universo en crecimiento, que atrae más y más anunciantes e inversiones, sea, también, víctima de los estafadores? Definitivamente no. ¡El fraude es la otra cara de la medalla del éxito!

También parece importante recordar que el contexto general del mundo de los negocios tiene influencia sobre el fraude. La cultura de resultados (en detrimento del análisis de los medios), la presión constante para hacer bajar las tarifas (uno puede apuntar sólo a las mujeres embarazadas de Madrid, a un euro el CPM), la deshumanización de las relaciones, etc., son otro tanto de incitaciones al fraude. Evidentemente ningún segmento de negocio ha logrado eliminar completa y definitivamente el fraude. Tan pronto como cerramos una brecha, otra se abre. Y lo digital no lo logrará tampoco.

Dicho esto, es esencial luchar firmemente contra el fraude, reducirlo, por supuesto, pero también «salvar el honor» de la profesión. ¡No todos los deportistas están dopados, no todos los políticos son corruptos, no todos los actores digitales son estafadores!

Es una tarea diaria y todos los integrantes de la cadena digital (anunciantes, agencias, editores, diversos proveedores de servicios, etc.) deben abordarla cuestionándose a sí mismos, analizando sus prácticas, etc. Los fraudes surgen a menudo de normas imprecisas que dejan a los defraudadores un margen de maniobra: un contrato que no especifica suficientemente los productos a entregar, una organización que no distingue entre los que controlan y los que compran, etc. Esto permitirá, si no eliminar el fraude, al menos diferenciarlo de las malas prácticas. Y es absolutamente necesario lograr esta diferenciación, para que el grueso de nuestros esfuerzos en la lucha contra el fraude se dirija a los objetivos correctos.

Por eso la CPA ha decidido dedicar este libro blanco exclusivamente a las técnicas de fraude. Para que todos puedan identificar claramente las áreas de debilidad que deben ser vigiladas. Tal y como vas a leer, existen soluciones para limitar el fraude. A menudo provienen del sentido común y no son tan complicadas de implementar.

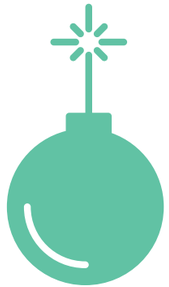
En un momento en que todo el mundo (medios de comunicación, anunciantes, etc.) parece descubrir y sorprenderse de la existencia de fraudes en el mundo digital, nos pareció importante aportar elementos tangibles y racionales sobre el tema. La encuesta que realizamos entre los anunciantes y las agencias sobre el fraude en *Display* es un paso en esta dirección.

Por lo tanto, esperamos que este libro blanco le ayude a comprender los sistemas de fraude para que pueda protegerse mejor de ellos en su negocio. Ciertamente no es la construcción de un muro a prueba del fraude, sino una piedra fundamental que sentimos que era necesario colocar.

Christophe Bosquet
Presidente del Colegio de Tecnologías Marketing del CPA
effinity

EDITORIAL

EL FRAUDE EN EL ÁREA DE LA PUBLICIDAD DIGITAL SERÍA HOY EN DÍA LA ACTIVIDAD ILEGAL MÁS LUCRATIVA DEL MUNDO DESPUÉS DE LAS DROGAS. CUANDO SE TRATA DE FRAUDE EN LO DIGITAL, LA REACCIÓN UNÁNIME ES PENSAR EN LOS PROBLEMAS DE SEGURIDAD INFORMÁTICA Y FALSIFICACIÓN DE DATOS PERSONALES Y FINANCIEROS.



Sin embargo, hay un fraude digital menos conocido... cuyo impacto financiero es mucho mayor: el fraude en la publicidad digital.

La Federación Mundial de Anunciantes (WFA) estima que el impacto podría ser del orden del 30 al 40% de las inversiones en medios digitales mundiales en 2025, es decir una suma del orden de 150 mil millones de dólares.

Sin esperar hasta el 2025, White Ops, empresa de seguridad cibernética americana especializada en el fraude publicitario ha revelado en diciembre de 2016 la existencia de un extenso sistema de estafa montado por hackers rusos. Creando sitios falsos, impulsados por un tráfico falso, la red de Methbot habría generado hasta cinco millones de dólares al día. En términos prácticos, la estafa funciona de la siguiente manera: la red Methbot ha tomado el control de más de 500 millones de direcciones IP. A cada una de estas direcciones IP, los hackers también han asignado *bots*, programas diseñados para imitar los hábitos de navegación de un humano (reproducción de un video, carga de una página).

Al mismo tiempo, los operadores rusos se hacen pasar por 6000 sitios de primer nivel: medios de comunicación como CNN y Fox News, las redes sociales como Facebook o sitios de marca como Pokémon.

Los anunciantes fueron engañados para que compraran espacio en estos sitios a través de Ad Exchanges con CPM elevado, que van de 3 a 37 dólares.

Algunos anunciantes entendieron el impacto de fraude digital y están tomando medidas para combatirlo.

En cuanto al tema del fraude, además de las cifras dadas por la prensa, se añaden los temas de la transparencia y la medición.

El principal anunciante del mundo, Procter & Gamble, pidió a sus agencias en febrero de 2017 que realizaran un esfuerzo para ser transparentes sobre las trampas que distorsionan las cifras de la publicidad online. P&G anunció 5 medidas para combatir la opacidad, incluida la adopción de una norma de visibilidad única desarrollada por el Media Rating Council y el uso de la certificación *Trustworthy Accountability Group* para prevenir las prácticas maliciosas y/o ilegales.

AL MISMO TIEMPO, EL DECRETO DE APLICACIÓN DE LA LEY SAPIN EN LA PUBLICIDAD DIGITAL FUE FINALMENTE ADOPTADO EN EL BOLETÍN OFICIAL DEL ESTADO FRANCÉS EL 9 DE FEBRERO DE 2017.

LA LEY SAPIN (FRANCIA)

El deseo de publicar esta ley en Francia era aún más intenso tras la revelación en junio de 2016 de las prácticas de agencias de medios en Estados Unidos y el consiguiente escándalo. Asimismo, el debate venía alimentado regularmente por los descubrimientos de fraudes publicitarios de gran calado como el que sacó a la luz White Ops a finales de diciembre de 2016 (Methbot).

Este decreto confirma la aplicación a la publicidad en línea de los principios de transparencia de la ley Sapin de 1993 sobre las transacciones publicitarias realizadas en los medios de comunicación franceses. Se exige a los vendedores de espacios lo siguiente:

El artículo 2 de dicho decreto estipula la información que debe incluir el informe que el vendedor de espacios publicitarios debe transmitir al anunciante:

«La fecha y los emplazamientos de la difusión de los anuncios, el precio total de la campaña, así como el precio unitario facturado por los espacios publicitarios.»

El artículo 3 define el proceso automatizado de espacios publicitarios en internet para actuar contra el fraude de clic publicitario resultante del uso de bots destinado a falsear los datos de tráfico.A partir de ahora, el vendedor deberá transmitir al anunciante un informe que incluya: «la información que permita garantizar la ejecución efectiva de los servicios y de sus características: la información que permita garantizar la calidad técnica de los servicios; la información acerca de los medios previstos para proteger la imagen de la marca del anunciante»

SE SOSPECHA QUE FACEBOOK Y GOOGLE, PRINCIPALES ACTORES DEL MERCADO, NO SON TRANSPARENTES EN SUS MEDICIONES DE AUDIENCIA. EL RENDIMIENTO DE LA PUBLICIDAD DIFUNDIDA EN GOOGLE Y FACEBOOK ESTÁ AUTORREGULADO: NO HAY TERCERO DE CONFIANZA.

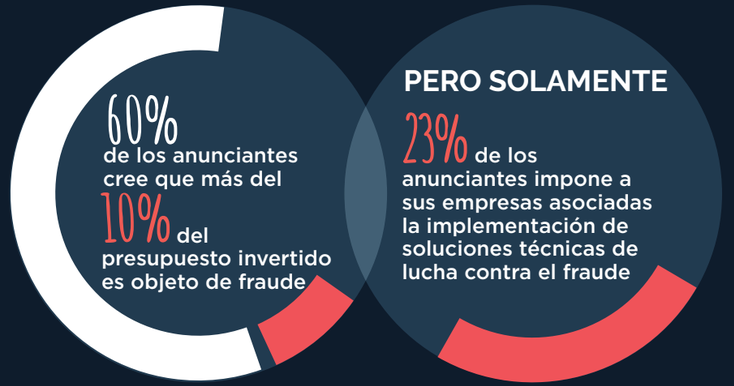
Google

Google: en 2015 investigadores europeos llevaron a cabo un experimento que demostró que YouTube (es decir, Google) facturó a los anunciantes incluso cuando su publicidad era vista por un robot en vez de por un humano.
Esto sucedió a pesar de que YouTube era perfectamente capaz de identificarlos como *bots*.
Todo ello hizo que se plantearan preguntas acerca de los intereses de YouTube en inflar artificialmente la audiencia, puesto que su modelo económico está directamente relacionado con el tráfico generado.

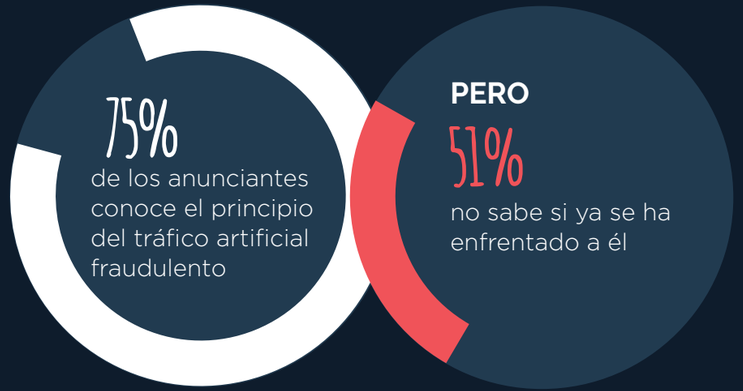
Facebook: Tras recibir críticas por numerosos errores cometidos en la medición de sus audiencias, la red social decidió ceder y abrirse a mediciones de terceras partes.
En numerosas ocasiones desde el verano de 2016 la plataforma fue cazada proporcionando errores en las mediciones de audiencia que comunica a las agencias y anunciantes que compran espacios publicitarios en la red social. A partir de ese momento, Facebook permitió a los anunciantes verificar la visibilidad de las impresiones *display* gracias a empresas asociadas como MOAT, IAS y Comscore.
Sin embargo, estos nuevos *partners* no *taggean* las páginas de Facebook de la misma forma que hacen con otros sitios. En una situación normal, la empresa de medición pone su *tag javascript* en la publicidad. A continuación, mide cada 100 milisegundos si el *banner* es visible y en qué medidas. Pero no en Facebook. El *partner* que mide se contenta con reprocesar y analizar datos en bruto que le transmite Facebook.

En el marco de su Libro Blanco, el CPA ha llevado a cabo un estudio mediante un cuestionario acerca del estado del fraude en Display dirigido a anunciantes y agencias. Hemos recibido unas 100 respuestas a este cuestionario.
El tratamiento de las respuestas nos ha permitido extraer las siguientes conclusiones:

CONCLUSIÓN



EL TRÁFICO ARTIFICIAL



LOS ESPACIOS ARTIFICIALES

PARTE 1. VENDER UN ESPACIO FICTICIO

INTRODUCCIÓN

El fraude en la publicidad digital se divide en cuatro temas principales:

1) Falsos espacios

> Más del 40% de los anuncios facturados y difundidos en internet en realidad no son vistos por los usuarios, ya sea porque se colocan bajo la línea de flotación o porque no son humanos los que los están visualizando.

2) Falso tráfico

> Se estima que los *bots* son responsables del 42,2% del tráfico registrado en 2019.

3) Mal targeting

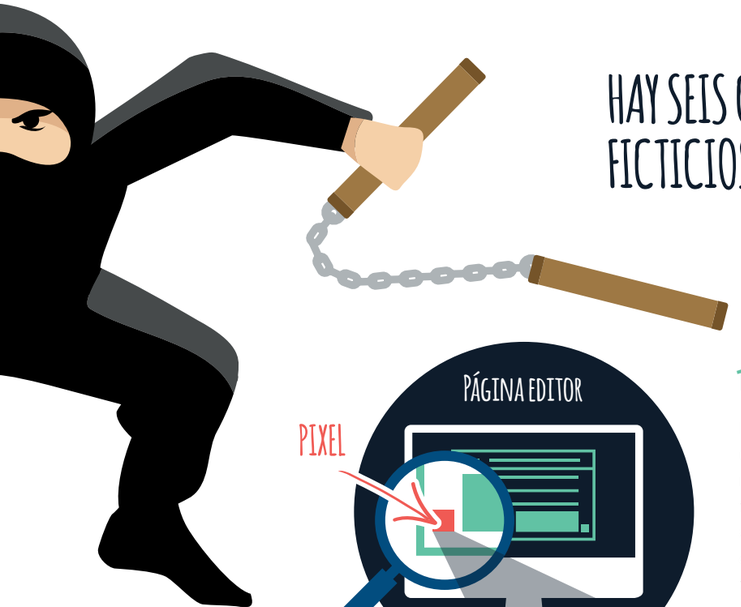
> Ciertos *targetings* propuestos, en base a criterios sociodemográficos o de intereses personales (edad, geografía, sexo, profesión, hobbies, etc.), no se corresponden con la realidad de los usuarios realmente expuestos a la campaña publicitaria.

4) Rendimientos falseados

> Algunos editores manipulan la navegación de los usuarios para aumentar sus rendimientos.

Los espacios ficticios son espacios publicitarios fantasma diseñados para engañar a las herramientas de Ad Serving haciéndoles creer que la publicidad se muestra correctamente

-como en cualquier sitio genuino- cuando en realidad o no lo está haciendo, o lo está haciendo de tal manera que se vuelve ineficaz o lo está haciendo ante *bots*. En resumen, se trata de técnicas que desproveen a la publicidad de su objetivo de informar con el fin de mantener sólo la generación de ingresos para el estafador.



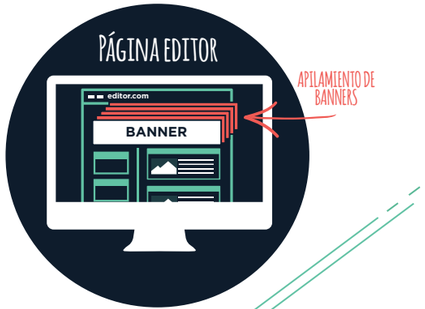
HAY SEIS CATEGORÍAS DE ESPACIOS FICTICIOS:

1. PIXEL STUFFING

El estafador reduce los anuncios a un solo píxel (tamaño 1x1 - invisible) que llama al *Ad Server* sin mostrar el anuncio correspondiente. Todas las funciones asociadas al *Ad Server* permanecen activas: se cuenta una impresión, se deja una *cookie* pero el usuario no ha visto nada. Esta técnica permite mostrar decenas de anuncios en una sola página generando grandes volúmenes de impresiones incluso en un sitio de poco tráfico.

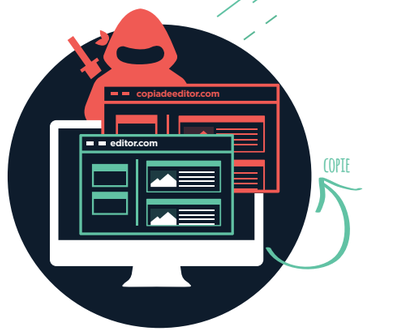
2. APILAMIENTO DE ANUNCIOS O AD STACKING

En un único espacio publicitario, el estafador apila anuncios unos sobre otros, una especie de milhojas digital. Cada *Ad Server* implicado considera que los anuncios se muestran y cobra a los anunciantes por esta difusión. Se dejan las *cookies* correctamente, mientras que solo el *banner* superior es visible para el usuario. Al igual que en la categoría anterior, se puede publicar múltiples anuncios y asegurarse unos ingresos en un espacio mínimo.
En la misma línea, el defraudador puede esconder *banners* detrás de una publicidad. Solo será visible dicha publicidad para el usuario.



3. SITIOS FANTASMA

Hay sitios fantasma que parecen sitios legítimos, pero están llenos de anuncios y son visitados casi exclusivamente por *bots*. El propietario del sitio - el botmaster - se registra como un difusor legítimo en las redes de afiliación o de SSP, pasa las fases de control de estos proveedores porque el sitio realmente existe y parece activo incluso si el contenido se copia a menudo de blogs o enciclopedias como Wikipedia. Una vez referido como un difusor, el sitio mostrará anuncios de diferentes anunciantes, pero no serán vistos por seres humanos, sino más bien por *bots*.



4. EL AUTO-REFRESH

Este método consiste en actualizar automáticamente el mismo espacio publicitario con un anuncio diferente cada vez.
Por lo tanto, el usuario ve todos los anuncios pero durante un tiempo irrisorio.

5. MALWARE EN MÓVILES (MOBILE DEVICE HIJACKING)

Hay aplicaciones que pese a haber sido validadas en las *appstores*, se ejecutan en segundo plano, muestran anuncios y hacen clic en ellos. Esto pasa con las aplicaciones cerradas e incluso sin haberlas abierto nunca. Pueden ejecutarse cuando el dispositivo arranca, cuando está bloqueado, etc. Los anuncios son invisibles para el usuario, pero los clics falsos y las impresiones generadas por estas aplicaciones pueden implicar grandes volúmenes. Estas aplicaciones establecerían hasta 1100 conexiones por minuto y se comunicarían con 320 redes publicitarias.

> El riesgo de fraude 0 no existe y puede provenir tanto del editor final como de los intermediarios. Controlar la cadena de valor reduciendo el número de intermediarios es un prerrequisito. Además, es esencial añadir herramientas de control independientes, así como evaluar con precisión la contribución real de los canales de marketing a las ventas finales.

Fabien Omont
Data & Attribution Manager
Oath:

6. ANUNCIOS OCULTOS EN APLICACIONES MÓVILES

Como en una página web, hay casos de fraude de apilamiento de anuncios o *banners* invisibles en una aplicación. A estos anuncios se les llama directamente desde el código de la aplicación sin que se muestren, no son visibles para el usuario.

PARTE 2. VENDER UNA AUDIENCIA FICTICIA

INTRODUCCIÓN

Una parte importante del fraude publicitario en internet se hace a través de *bots*. Pueden ser más o menos sofisticados y no todos son maliciosos.
Algunos *bots* sirven a la red de manera positiva, por ejemplo para mejorar los motores de búsqueda.
Estos se declaran con tecnologías de colecta de datos para no ser contados en los diversos informes, en particular gracias al archivo «robots.txt».

Los *bots* maliciosos, por otro lado, tienen el objetivo de crear audiencias ficticias y simular el comportamiento humano para generar visitas al sitio, impresiones o clics en anuncios. Esta es la actividad de los piratas, a menudo organizados en redes, que usurpan las direcciones IP de los ordenadores con el fin de simular acciones publicitarias para hacerse con los ingresos.
Como en un remake de Terminator versión *adtech*, el *bot* es la pesadilla del comprador de espacios en medios. No tiene corazón, no tiene cerebro y sobre todo no tienen ningún potencial económico para llevarlo a la plataforma de pago para finalizar un pedido en un *e-commerce*. Sin embargo, los *bots* están por todas partes. Y no siempre de manera inútil.
Según un estudio de Imperva de 2019, los *bots* «malos» representan el 21,8% del tráfico de internet.

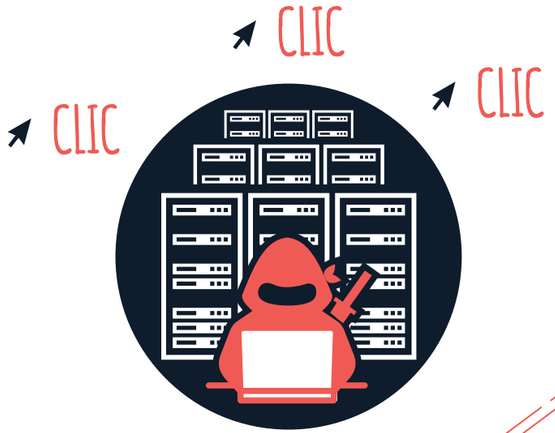
*http://robots-txt.com/

HAY TRES TIPOS DE BOTS FRAUDULENTOS, DESDE EL MÁS SIMPLE AL MÁS SOFISTICADO:

1. EL BOT INDEPENDIENTE

El objetivo de este tipo de *bots* es el de simular impresiones y clics en anuncios desde un simple ordenador. Los delincuentes que desarrollan este tipo de *bot* se centran en quienes no consideran el fraude una amenaza y que no han puesto en marcha herramientas de detección específicas. Si toman la precaución de no generar ingresos muy elevados, su actividad puede durar un tiempo.

Estos *bots* pueden imitar comportamientos humanos, como el movimiento del ratón, navegación por una sitio, visitas a distintas páginas, clics en diferentes enlaces, reproducción de vídeo... Son mucho más difíciles de identificar que otros *bots*.



2. EL BOT DATA CENTER

Este es más complejo y sólo puede ser operado por una organización con acceso a varios servidores para multiplicar las IP. Estos *bots* reproducen las acciones de los bots autónomos pero masivamente.

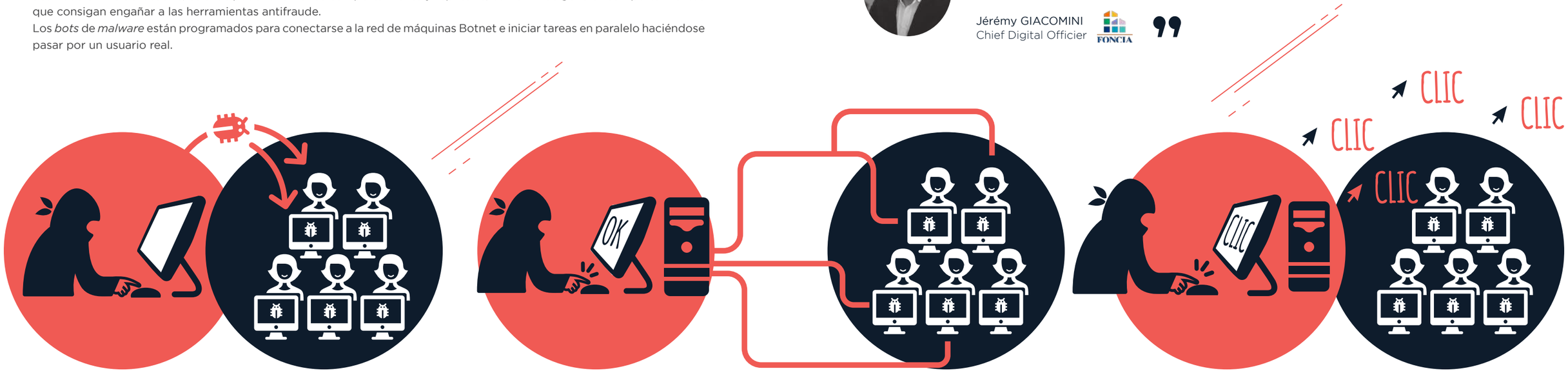
Los *data centers* permiten alquilar ordenadores por un tiempo, por lo que es posible utilizarlos durante un corto período de tiempo para usar estos *bots*.

3. BOTNET: LA RED DE BOTS MALWARE

El *malware* es un virus instalado en un ordenador. El interés del estafador, además del de tener el control absoluto de la actividad online del usuario, es el de poder analizar su comportamiento y replicarlo, con el fin de generar comportamientos que consigan engañar a las herramientas antifraude.
Los *bots* de *malware* están programados para conectarse a la red de máquinas Botnet e iniciar tareas en paralelo haciéndose pasar por un usuario real.

> Distinguimos entre dos tipos de fraude: fraude de impresión y fraude de clics. Foncia trabaja desde hace tiempo con actores de confianza, hay muy pocos casos de fraude. Cuando integramos un nuevo *partner*, hay una fase de prueba, si los resultados no aparecen, lo medimos de inmediato.

Jérémy GIACOMINI
Chief Digital Officier



LAS GRANJAS DE CLICS

En junio de 2017, una red fue desmantelada por las autoridades tailandesas después de descubrir una granja de clics compuesta por 500 teléfonos móviles que utilizaban 400000 tarjetas SIM diferentes

(fuente: Omicrono - 13/06/2017: https://www.elespanol.com/omicrono/tecnologia/20170613/personas-tarjetas-sim-iphone-falsear-likes/223478687_0.html).

Este tipo de dispositivo se utiliza principalmente para generar «Me gusta» en las redes sociales. Pero podemos imaginar tal infraestructura con el fin de generar falsos clics en los anuncios. Cabe señalar que los hechos imputados contra los implicados en este caso están relacionados con la ausencia de un permiso de trabajo y no con la naturaleza de sus actividades.

4. IFRAME STUFFING

Más allá de los *bots*, hay un método simple para generar tráfico ficticio llamando a una página o incluso a un sitio entero en un *iframe*, o «*inline frame*» («marco incorporado» en español). El *iframe* es un elemento HTML que permite llamar a una página dentro de otra página. Al definir un ancho y alto de 1x1 píxeles, esta página se vuelve invisible para el usuario.

Se carga todo el contenido de la página incorporada, incluidos los anuncios, pero de nuevo el usuario no ve los elementos, que se cargan en segundo plano. Por lo tanto, un editor sin escrúpulos puede engañar a un *Ad Server* multiplicando sus espacios publicitarios sin inundar su contenido con anuncios más o menos intrusivos.

PARTE 3. VENDER UN TARGETING FICTICIO

INTRODUCCIÓN

El targeting permite centrar las inversiones publicitarias para alcanzar un target específico.

El *targeting* puede ser geográfico, por comportamiento, contextual o sociodemográfico.
A veces, los *partners* no lo respetan, sea de manera voluntaria o no (agencia, *trading desk*, editor, proveedor de datos de terceros, etc.).
Esto se conoce como la alteración del *targeting*.

ESTOS SON ALGUNOS EJEMPLOS

1. FRAUDE EN EL TARGETING DE SEGMENTOS DE USUARIOS

Pongamos un ejemplo: en su campaña el anunciante quiere dirigirse a una audiencia en particular (por ejemplo: mujeres con alto poder adquisitivo que pretendan comprarse unos zapatos). El *partner* le hace creer que está haciendo *targeting* a personas en función de los criterios sociodemográficos y/o intencionales. En realidad, la campaña se difunde sin haber recurrido al *targeting*.
Para el anunciante, esto implica una inversión en medios que no corresponde a sus instrucciones iniciales, lo que puede afectar al rendimiento de su campaña.

¿Qué motiva este fraude?
Para el comprador de medios: justifica un CPM alto gracias al *targeting* de datos de terceros calificados pero sin utilizarlos, comprando así un espacio publicitario mucho más barato y aumentando mecánicamente su margen. Para el proveedor de datos: esto le permite aumentar de manera ficticia el precio y el volumen de sus segmentos.

2. FRAUDE EN LA DIFUSIÓN

El *partner* se compromete con el anunciante a difundir la campaña en una lista definida de sitios. Pese a esto, para reducir sus costes de compra, el *partner* difunde los *banners* en una lista más amplia y/o diferente de la lista predefinida. Así se corre el riesgo de que los *banners* se publiquen en sitios que no tengan afinidad con el *target*, o incluso que sean potencialmente dañinos para la marca en términos de imagen.

Hay que tener confianza con su *partner* y a su vez él tiene que tener confianza con los suyos. Lo cual es difícil dado el número de intermediarios. No creo en el *targeting* de perfiles (intereses / sociodemográficos) basado en datos externos porque se necesita frescura. Miro la diferencia entre el número de clics y el número de sesiones, la tasa de rebote y uso tanto como puedo un píxel de impresión propio.

Paulo Esteves
Chief Digital Officier

3. FRAUDE EN LA GEOLOCALIZACIÓN

El *partner* se compromete con el anunciante a difundir la campaña en una zona geográfica específica (país, ciudad, región...). Este tipo de *targeting* generalmente limita la potencia de la difusión para el *partner*. Puede ocurrir entonces que el *partner* difunda fuera de la zona definida para engordar el volumen de impresiones.

4. DOMAIN SPOOFING

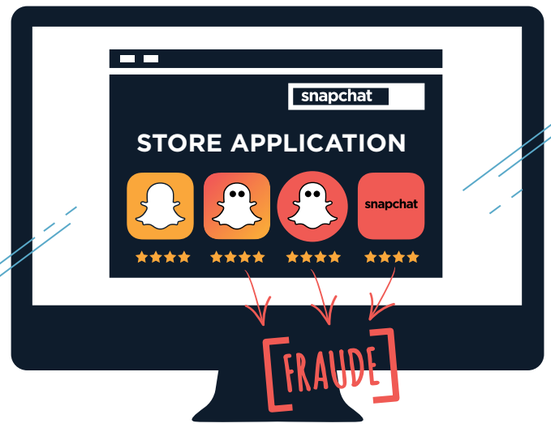
El *domain spoofing* es un fraude al cual algunos estafadores recurren en programática con el fin de usurpar el nombre de dominio de los sitios premium. La agencia tiene la sensación de que sus anuncios se publican en espacios de calidad cuando en realidad es al revés. Las impresiones se generan en sitios de baja calidad o incluso perjudiciales para la marca. El *domain spoofing* hace que la selección de sitios no funcione, hace que haya una malversación de los presupuestos de los anunciantes y los ingresos de los editores suplantados. El *domain spoofing* es probablemente el fraude más engañoso, el más lucrativo y difícil de detectar.

5. LA USURPACIÓN DEL DISPOSITIVO

Los emuladores son programas que permiten a los desarrolladores validar su trabajo emulando diferentes dispositivos móviles. Algunos estafadores utilizan estos emuladores y cambian los encabezados http del alojamiento de los emuladores para hacerse pasar por cualquier otro dispositivo y generar impresiones falsas.

6. LA USURPACIÓN DEL NOMBRE DE UNA APP

Los nombres de las apps puedes cambiar, por lo que es importante hacer un seguimiento de aquellas a las que estás expuesto por su *Bundle ID*, no por su nombre.



PARTE 4. VENDER UN RESULTADO FICTICIO

INTRODUCCIÓN

Para valorizar correctamente los espacios vendidos, lo mejor es mostrar un buen rendimiento en las herramientas de atribución utilizadas por los anunciantes. Y para estar seguro de rendir bien, la forma más fácil es asegurarse de que los números muestren la verdad "verdadera". Lo último es el «robo de conversión» mediante la manipulación de la herramienta de tracking utilizada.

El mayor caso sospechoso que ha estallado hasta la fecha es el caso Steelhouse/Criteo (ver recuadro) pero estas prácticas, muy escasas en los últimos años, son cada vez más comunes y, sobre todo, más sofisticadas. Las estafas de targeting también son comunes. Targetizar a los usuarios que ya sabemos que van a comprar de todos modos es una buena manera para que un vendedor valorice el espacio que vende...
Para acabar, los viejos rockeros nunca mueren. Pagar al usuario para que haga lo que el anunciante espera sigue siendo un clásico desde el comienzo de la publicidad digital hace veinte años.

EN JUNIO DE 2016, CRITEO PRESENTÓ UNA DENUNCIA CONTRA STEELHOUSE. SI BIEN LA QUEJA SE DESCRIBE COMO «CLICK FRAUD» (FRAUDE DE CLICS), EN REALIDAD SE TRATA DE UNA PRESUNCIÓN DE FRAUDE A LAS HERRAMIENTAS DE ATRIBUCIÓN.

Criteo se siente engañado. Así es, los equipos de Criteo consideran que un gran número de ventas se atribuyeron por los anunciantes y sus herramientas de *tracking* a Steelhouse por acciones fraudulentas de Steelhouse.

Este caso es interesante porque es de un nuevo tipo.
Un vendedor de tráfico al que roba conversiones (que deberían serles atribuidas) otro vendedor de tráfico es un caso inédito en el marketing digital.

Pero los aspectos empresariales y legales no son los únicos aspectos interesantes de este tema. De hecho, técnicamente, hay que tener en cuenta varias peculiaridades:
- Los riesgos asociados a la instalación de *javascript* de terceros en las páginas del anunciante. Esto ilustra lo que se puede hacer con un *javascript* en una página web.
- La dependencia de los anunciantes y sus proveedores de tráfico a las herramientas de atribución y, por lo tanto, la tentación de estos últimos de intentar cambiar las cifras a toda costa.
- El supuesto ingenio de los equipos de Steelhouse que parecen haber montado una estratagema optimizada de manera iterativa.

Con Steelhouse y Criteo llegando a un acuerdo a finales de octubre de 2016, el público en general nunca conocerá la última palabra de la historia, pero merece la pena leer la documentación legal escrita por los abogados de ambas compañías.

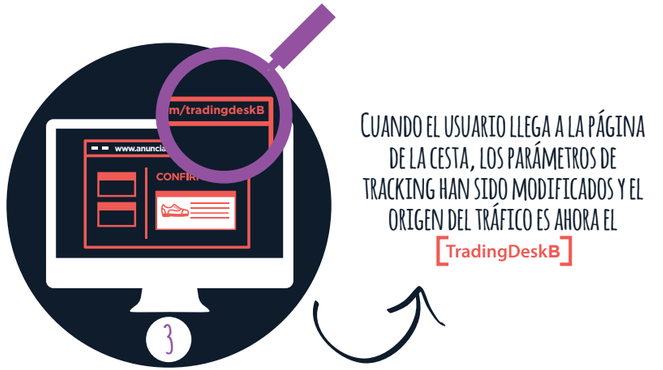
1. ALTERACIÓN DEL TRACKING (UTM SOURCE)

La alteración del *tracking* es un método de fraude cuyo objetivo es cambiar el resultado de una campaña para mejorar la percepción de los resultados. Este tipo de fraude requiere engañar a las herramientas de *tracking* para que asignen conversiones a una campaña en lugar de a otra.

El método más conocido son las herramientas de analítica y atribución que utilizan parámetros en las URL. Estos son visibles y comprensibles para los piratas. Es el caso de las etiquetas *utm* de Google Analytics, como *utm-source* y *utm-medium*. Aquí el pirata buscará reemplazar el contenido de la variable con el nombre de la fuente de tráfico que está comercializando. Esto le permite optimizar el número de conversiones asociadas al tráfico que genera y así mejorar significativamente sus posibilidades de seguir vendiendo tráfico al anunciante en cuestión, o incluso permitirle aumentar sus precios.

Técnicamente, el pirata explota un código *javascript* que ha proporcionado al anunciante y que el anunciante ha instalado en sus páginas. Este código *javascript* permite al pirata cambiar la URL actual cuando el usuario hace clic en la página de un anunciante. De este modo, el hacker cambia el contenido de la configuración que indica la fuente de tráfico de la visita (por ejemplo, *utm-source*). Así, para cambiar la url, puede utilizar capas transparentes que instala en las páginas del sitio del anunciante gracias a su *javascript* y en las que el usuario hará clic sin su conocimiento.

Este método es difícil de detectar por parte del anunciante. Puede ser detectado por otros proveedores de tráfico porque corren el riesgo de ver el número de ventas atribuidas a ellos fluctuar bruscamente. El caso más conocido de alteración del *tracking* es la batalla legal entre Criteo y Steelhouse (ver recuadro).



2. ADD-ONS

Los *add-ons* o complementos son programas adicionales que se puede agregar a un navegador. Pueden ser de varios tipos: *adblockers*, herramientas de reembolso, herramientas de descarga de vídeo, *plug-ins* sociales, herramientas de depuración de errores... Si bien la mayoría de estos complementos son útiles e inofensivos, el objetivo de algunos otros es alterar la publicidad visualizada por un usuario e incluso crear nuevos espacios.

Se han encontrado más de 130 extensiones maliciosas y 4712 sospechosas de serlo en el navegador Chrome, asociadas con varios tipos de fraude: robo de datos (identificadores y contraseñas), redirección a anuncios fraudulentos o piratería de cuentas de redes sociales. El usuario no puede percibir el aspecto fraudulento de la extensión, que para él es un servicio que se le ofrece. El comportamiento malintencionado de estos complementos solo se desencadena en determinadas páginas seleccionadas previamente por los desarrolladores.

Extensiones de este tipo realizan llamadas a las API del navegador para acceder a varios permisos (consulta web, cambio de tráfico, redirección no deseada, inyección de código *javascript* en páginas de internet...). Sin embargo, el usuario debe dar permiso a la extensión para que pueda beneficiarse de los datos. Algunas extensiones contienen etiquetas de ubicación que les permiten comunicar a un servidor remoto todo el historial y los datos de navegación del usuario afectado. A partir de ahí, la URL se puede cambiar para depositar *cookies*, por ejemplo. Las extensiones pueden reemplazar los anuncios con otros o poner publicidad en sitios que no tienen espacios para ellos. Se puede generar falsos clics o llamadas de visualización, así como la instalación invisible de otros *malwares*.

> El rendimiento es el criterio para descartar a los estafadores. Hacemos pocas campañas programáticas porque el CPM es demasiado alto y el rendimiento es demasiado bajo.

Thomas Hadjadj
Digital Acquisition Marketing Manager
Head of Display Europe

3. RETARGETING DISFRAZADO DE TARGETING

El anunciante llama a un *partner* para implementar una estrategia de *targeting* con el objetivo de llegar a un nuevo público que pueda comprar productos o comprar servicios. Esto implica la exclusión de todos los visitantes de estas campañas.
En la práctica, gracias a los elementos de *tracking* proporcionados al anunciante para medir el rendimiento, el *partner* puede identificar en algunos casos a los visitantes del sitio para hacerlos *retargeting*. Dicho *retargeting* permite aumentar drásticamente el rendimiento de la campaña en términos de tasas de clics y conversiones.
Las razones que incitan al *partner* a cometer este fraude son diversas. En caso de competir con otro *partner*, el objetivo sería mejorar el rendimiento para ser seleccionado por el anunciante. Otra razón es que la reducción del coste de adquisición (CAC) puede, en algunos casos, permitirle obtener nuevos presupuestos.
El impacto para el anunciante es una lectura errónea del rendimiento de sus campañas. Además de solicitar en exceso a los visitantes del sitio, esta estrategia de prospección no genera nuevos visitantes.
Control con herramientas de *tracking*: para detectar el *retargeting* disfrazado de *targeting*, es necesario estudiar la tasa de nuevos visitantes a través de herramientas de *tracking* y realizar un seguimiento a lo largo del tiempo.

4. EL TRÁFICO INCENTIVADO

Este es quizás el fraude más antiguo en publicidad digital. Al principio de los sistemas de enlaces patrocinados, ¡los piratas informáticos ya estaban revendiendo tráfico incentivado a Google o Yahoo! Eso fue hace casi 15 años y este fraude continúa.

El tráfico incentivado puede adoptar la forma de *pay-to-click* (o *crowd sourcing*) y de *incentivised ad network*. En el caso de los *pay-to-click*, se paga a los usuarios para que hagan clic o lean anuncios. En cuanto a la *incentivised ad network*, se anima a los usuarios a hacer clic en los anuncios a cambio de puntos en el programa de fidelización, cupones, *bitcoins*, etc. El tráfico incentivado permite al *partner* aumentar las estadísticas y obtener tasas de clics o volumen de visitas que parecen ser interesantes para el anunciante.

Por su parte, el anunciante no tiene una buena lectura del rendimiento real de sus campañas. Debe utilizar una herramienta de atribución de última generación para detectar el tráfico que recurren a proveedores de tráfico incentivado (ver esquema).

PARTE 5. LAS MALAS PRÁCTICAS

INTRODUCCIÓN

Dentro de toda la diversidad de formatos publicitarios, hay un número de ellos que se le impone de una manera más o menos brutal al usuario.

Esto reduce la capacidad de escapar del anuncio. Al usuario se le obliga de malos modos a ver la publicidad, es decir, se manipula a las personas.

Hay una diferencia de madurez significativa entre los anunciantes: los que no saben que hay que *trackear* y los que se dedican a cazar a los *bots* inteligentes. Hay que evitar al máximo los vicios de forma en los contratos, sobre los visitantes únicos no hay nada que estipule que deban ser humanos.

Alexandre Schont
Responsable Business Development

TABMO
CREATIVE MOBILE DSP

1. INTERSTITIAL

El *interstitial* es una página publicitaria que cubre completamente la pantalla en el móvil. Por lo general, aparece cuando se abre una app o cuando navegas entre dos páginas. Sin embargo, hace falta un clic para cerrarlo, que puede a veces ser difícil de hacer, dado el tamaño de la equis que permite cerrar el formato.
Es un formato muy intrusivo, la dificultad para cerrarlo explica sus altas tasas de clics. Además, cada vez más agencias, editores y *Ad Exchanges* se niegan a difundir este formato.

2. EL VÍDEO QUE NO SE PUEDE SALTAR

El *pre-roll* es un anuncio de vídeo de unos segundos que aparece antes de ver un vídeo de contenido. Este es un formato que suele durar entre 10 y 30 segundos. Formato intrusivo, la peculiaridad del vídeo que no se puede saltar es precisamente esa, que no se puede saltar. El usuario se ve obligado a ver el anuncio al completo, antes de que aparezca el contenido deseado. A veces incluso, el anuncio se detiene cuando el usuario visita otro contenido al mismo tiempo.

3. BANNER TIPO SKIN COMPLETAMENTE CLICABLE

El *banner* tipo *skin* es un formato publicitario que se utiliza a menudo cuando hay un evento, que al principio aparecía sólo en la homepage de un sitio, pero que desde hace un tiempo se utiliza también en el resto de las páginas. La ausencia de call to action en la parte superior y en los laterales de la página significa que los clics realizados por un usuario no siempre son voluntarios, lo que hace que estos se desvíen del contenido por el que habían entrado en el sitio.

4. SITE UNDER

Aunque este método se ha utilizado cada vez menos en los últimos años, sigue siendo una técnica de generación de tráfico masivo.
Consiste en abrir la página de un anunciante en una nueva ventana del navegador y debajo de la ventana activa. De este modo, el usuario no verá dicha ventana hasta que cierre todo y deje de navegar.

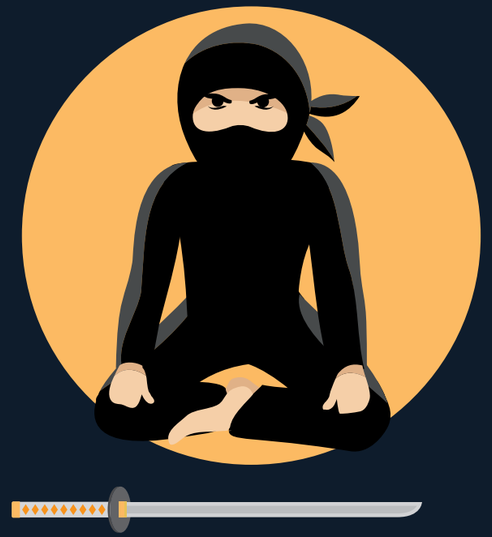
5. FOOTER EXPAND

El footer expand puede dejar una *cookie* posclic al desplegarse. Aunque esta forma de proceder puede estar en el límite, es principalmente el resultado de un imperativo técnico. Conviene pasar por una landing page en tales casos para evitar encontrar cierta confusión en los informes.

6. LA NO VISIBILIDAD DE LOS BANNERS

Los espacios publicitarios pueden estar fuera de la pantalla del usuario sin que esto tenga un propósito fraudulento, sino más bien que sea una manera suplementaria de monetizar páginas que pueden ser largas.
La IAB y el MRC han establecido un estándar para el mercado que consiste en contar un *banner* como visible si más del 50% de sus píxeles se muestran en la pantalla durante más de un segundo.

PARTE 6. LOS MEDIOS PARA LUCHAR CONTRA EL FRAUDE



* Usar herramientas de Analytics que muestren todo el funnel de conversión (evitar las herramientas gratuitas que no estén completas)
**Asegurarse de que todo el mundo hable el mismo idioma, entienda también los KPI y entienda los objetivos de la campaña

1. PROTECCIÓN LEGAL

Con el fin de protegerse legalmente y poder ir a por el proveedor en caso de incumplimiento de los compromisos, se debe prestar especial atención al contrato para plasmar ahí dichos compromisos.

Por ejemplo, los objetivos y plazos esperados deben estar claramente definidos y especificados en el contrato con el proveedor (agencia, administración u otro). Si el anunciante desea imponer el uso de herramientas de control y verificación (control de espacios y visibilidad), esto también debe especificarse en el contrato.

Por lo tanto, podremos encontrar limitaciones en el contrato, como poder acceder a las fuentes de inventarios y la calidad de su audiencia, especificar si la extensión de audiencias está autorizado, poder conocer los gastos reales en cada una de las fuentes o tener que respetar una tasa de nuevos usuarios o clientes en caso de que el *retargeting* no esté abierto.

EN FRANCIA - LEY SAPIN: PUBLICIDAD PROGRAMÁTICA

El decreto de aplicación No 2017-159 del 9 de febrero de 2017 que aclaró recientemente la ley relativa a la prevención de la corrupción y la transparencia de la vida económica y los procedimientos públicos conocido como la «Ley Sapin» (Ley 93-122 de 29 de enero de 1993) para, entre otras cosas, tener en cuenta las nuevas prácticas de intermediación en la publicidad programática.

EN RESUMEN, LOS TRES PUNTOS MENCIONADOS:

I - La inclusión de la publicidad digital y las prácticas de compra programáticas en el ámbito de aplicación de la Ley Sapin francesa. La ley ahora se aplica formalmente a las actividades de optimización del targeting publicitario en línea.
Los medios digitales como soporte publicitario y las prácticas de intermediación a través de sistemas automatizados están ahora expresamente cubiertos por la Ley Sapin.

II - Transparencia en la publicidad digital: obligaciones de presentación de informes.
El decreto impone obligaciones específicas de presentación de informes en materia de publicidad digital.

III – Las derogaciones al campo de aplicación territorial
El decreto no se aplica a los soportes (y sus agencias) establecidos en otro Estado miembro de la Unión Europea o que haga parte del Espacio Económico Europeo, siempre que estén sujetos a «obligaciones equivalentes» de presentación de informes, en virtud de disposiciones nacionales.

Ten en cuenta que el decreto dio tiempo a los actores a adaptarse, ya que las disposiciones del nuevo decreto empezaron a aplicarse el 1 de enero de 2018.

2. LA METODOLOGÍA

Antes de lanzar una campaña digital con un *partner*, es importante respetar varios pasos para poder seguir los resultados correctamente y garantizar que se respeten las expectativas.
El primer paso es crear informes que permitan realizar un seguimiento y supervisar.
Estos informes ayudarán a encontrar indicadores como:

- Tasa de clics
- Tasa de rebote
- Número de páginas vistas
- Tiempo invertido en el sitio
- Tasa de nuevas sesiones
- Tasa de transformación
- Tasa de nuevos clientes
- Distribución del origen del tráfico

El segundo paso es imponer el uso de tu herramienta de analítica para que puedas alimentar este informe con el mejor nivel de granularidad:

- Por campaña
- Por fuente de inventario
- Por soporte

A continuación, podrás analizar los resultados en este informe comparando permanentemente los resultados de las diferentes campañas para poder resaltar resultados anómalos.

3. LA IMPORTANCIA DE LA ORGANIZACION

La organización de los equipos del anunciante es un punto clave en la lucha contra el fraude.
Al igual que en las funciones de control de riesgos de mercado de los bancos, hay que diferenciar a la persona responsable de la campaña (la que contrata con los medios) de la persona que controla los resultados.

Aunque los niveles pueden variar, hay que internalizar al máximo las expertises para poder hablar el mismo idioma que los *partners* y poder seguir sus acciones.
Esta *expertise* debe tener un poder de decisión más importante que la dirección de compras en la asignación presupuestaria para no dejar el coste como único elemento que tener en cuenta.

4. LA TECNOLOGÍA

La última categoría concierne a las tecnologías de control del fraude.
Algunas tecnologías te permitirán supervisar la visibilidad de las impresiones de tu campaña. Ya sea en ordenadores o en móviles, esto permitirá cubrir diferentes casos de fraude.

Otras tecnologías te permitirán beneficiarte de la puesta en común de la vigilancia antifraude.
Estos *partners* tecnológicos mantienen listas de direcciones IP o de sitios en la lista negra (un poco como un antivirus mantiene y alimenta constantemente una lista de virus).
La detección se basa en algoritmos o estudios humanos:

- Detección de irregularidades para detectar comportamientos anómalos característicos de los *bots* (velocidad de navegación anómala, patrones de navegación recurrentes ...)
- Análisis del navegador: los *bots* utilizan falsos navegadores. Mediante un *script* implementado en el *Ad Server*, la herramienta analiza en tiempo real las características del navegador que se utiliza para vincularlas a características conocidas. Los parámetros diferentes o faltantes permiten identificar comportamientos fraudulentos.
- Estudio preliminar realizado por ingenieros y detección de «firmas» de *malware* o *bots*
- Observación proactiva de foros y comunidades de estafadores

En el caso de las campañas para tu aplicación para móviles, la tecnología te permitirá identificar el falso tráfico mediante el análisis de:

- Direcciones IP: si la misma dirección IP aparece con demasiada frecuencia en las descargas
- ID de dispositivo: si el mismo ID de dispositivo es responsable de varias descargas
- El nombre de los móviles («iPhone de Víctor", etc.): si el mismo nombre aparece varias veces
- Tipos/marcas de móviles: si se genera un gran volumen de descargas en un solo tipo de teléfono
- El tiempo entre el clic y la instalación: si es demasiado corto

Se identifica el tráfico desviado, es decir, el de calidad no deseada, mirando:

- La hora media de la acción o el uso de VPN: para comprobar la zona horaria
- Móviles con jailbreak: para identificar el tráfico no contabilizado por las *appstores*
- Tasas de conversión posteriores a la instalación dentro de la aplicación: para identificar el tráfico incentivado

Los principales actores en este campo son:

Se aconseja consultar el panorama de las herramientas técnicas contra el fraude (en inglés):
https://headerbidding.co/ad-fraud-detection-companies/
Para garantizar su fiabilidad, el único criterio hasta la fecha es la acreditación del *Media Rating Council* (MRC), una asociación estadounidense independiente cuya misión es garantizar la validez y eficacia de las herramientas de medición de audiencia.

En el caso de un presupuesto al CPM, requerimos que nuestros *partners* de *Display* utilicen una solución como IAS o Adloox.
Para controlar el targeting y evitar el ad stacking, confiamos en la analítica web para comprobar: tasa de rebote, tiempo invertido en el sitio, número de vistas de página, origen de la IP, perfiles de usuarios.
Para limitar el fraude, utilizamos deals garantizados (programática garantizada).

Grace Paynot
Responsable Marketing Digital,
CRM et Communication

PSA BANQUE

ADS.TXT

«En 2017, la IAB (*Internet Advertising Bureau*) lanzó la iniciativa ADS a través del IAB Tech Lab. TXT (ADS por *Authorized Digital Sellers* -Vendedores Digitales Autorizados-), que se materializa en forma de un archivo de texto colocado en la raíz de un dominio donde hay espacios publicitarios y que especifican sus identificadores de vendedor en los diversos mercados, así como diversas informaciones que permiten a los compradores asegurarse de que están comprando de verdad en el dominio elegido y no en un sitio haciendo *domain spoofing*.

Esta iniciativa es un paso en la dirección correcta y sin duda ayudará a hacer el ecosistema más transparente. Más información:
https://iabtechlab.com/ads-txt-about/

Ad-Exchange*:

El *Ad Exchange* es una plataforma automatizada para vender y comprar espacios publicitarios en internet. Conecta a compradores (DSP, agencias de publicidad, agencias de medios o directamente anunciantes) y vendedores (SSP, editores, redes o agencias de publicidad).

Los *Ad Exchanges* son uno de los componentes técnicos fundamentales del marketing programático. (fuente wikipedia)

Un *Ad Exchange* es una plataforma automatizada para la compraventa de espacios publicitarios de internet en el que se encuentran los que buscan espacios (anunciantes, agencias de medios y redes de *retargeting*) y lo que los ofrecen (editores, redes, agencias). En un *Ad Exchange*, la actividad de compraventa de espacios publicitarios se realiza generalmente en RTB.

Un *Ad Exchange* permite automatizar casi por completo las fases de negociación/compra e implementación de las campañas. En un *Ad Exchange* se puede configurar una campaña sin que en ningún momento haya contacto directo entre el vendedor y el comprador de espacio publicitario. Por lo tanto, el objetivo de un *Ad Exchange* es reducir los costes de explotación del mercado.

Un *Ad Exchange* se financia mediante una comisión por los intercambios muy inferior a la que normalmente cobra una agencia y posiblemente por las tasas de registro de los usuarios.

Como parte de una plataforma automatizada, los editores establecen un precio mínimo para sus diferentes espacios de publicidad disponibles y posiblemente un filtro para los anunciantes aceptados. Los anunciantes o agencias crean sus campañas eligiendo sus formatos, criterios de *targeting* y un precio de subasta al CPM o, aunque sea más raro, al CPC.

El *Ad Exchange* compara la oferta y la demanda en tiempo real y según el caso puede difundir campañas en tiempo real impresión por impresión o por bloques de impresiones.

SSP*:

SSP son las siglas de *Sell Side Platform* o *Supply Side Platform*. Una SSP es una plataforma para que los editores automaticen y optimicen la venta de sus espacios publicitarios.

Estas plataformas son utilizadas por los principales editores para comercializar espacios que no han podido ser comercializados de manera tradicional por su agencia interna o externa y posiblemente por los editores más pequeños para comercializar todo su inventario publicitario.

Las SSP difunden el inventario disponible de sus editores a los *Ad Exchanges* del mercado y posiblemente a las *Ad Networks* y otros DSP.

Las SSP más avanzadas funcionan en tiempo real. Cuando se llama a un espacio publicitario al ver una página en un sitio de editor, la plataforma busca la mejor oferta realizada para ese tipo de ubicación y de perfil de visitante detectado y difunde automáticamente el anuncio correspondiente.

Las SSP normalmente están destinadas a reducir la proporción de elementos no vendidos y a fomentar un aumento del CPM de los editores que las utilizan.

DSP*:

DSP son las siglas de *Demand Side Platform*. Una plataforma DSP es un servicio que permite a los anunciantes, *trading desk* y agencias optimizar sus compras de espacio de publicidad *display*.
La compra por una plataforma de optimización se realiza principalmente en los diversos *Ad Exchanges* del mercado. Las plataformas DSP funcionan generalmente en tiempo real en una lógica RTB. Cuando una campaña se programa y define a través de los criterios de *targeting* de un comprador, la plataforma de optimización busca las impresiones disponibles al mejor coste.
Una plataforma DSP también puede realizar adaptaciones durante la campaña para seleccionar creaciones, medios y criterios de *targeting* que garanticen el mejor retorno de la inversión en función de los objetivos de la campaña (clics, conversiones, etc.). Algunas herramientas llegan a analizar el contenido y las cantidades de ventas generadas en su proceso de optimización.
Las DSP son la contraparte para los compradores de las SSP para los editores.

Extensión de audiencia:

La extensión de audiencia (*audience extension*) es la práctica por la cual un sitio cuya audiencia es especialmente buscada por los anunciantes y que generalmente vende todo su espacio publicitario puede ofrecer a un anunciante llegar a su audiencia habitual a través de una red especializada.
La extensión de audiencia se basa en los mismos principios que las técnicas de *retargeting*.

*Trading Desk**:

Un *Trading Desk* es, en el campo de la publicidad en internet, una estructura que se encarga de la compra de espacio publicitario en los *Ad Exchanges* en nombre de los anunciantes. Los servicios de un *Trading Desk* se prestan desde una plataforma técnica (DSP y desarrollos específicos) y de un equipo técnico y de marketing especializado en la compra de espacios RTB.
En general, el *Trading Desk* cortocircuita las *Ad Networks* o agencias publicitarias haciendo la compra directamente en los sitios de editores o *Ad Exchanges* (*marketplaces* publicitarios) utilizando la mayoría de las veces el RTB. El *Trading Desk* optimiza la compra de publicidad mediante la integración del análisis del rendimiento y el posible uso de diferentes datos (datos de primera parte, datos del editor, datos de tercera parte). Por lo tanto, no busca necesariamente el CPM más bajo.
La persona encargada de planificar y optimizar las campañas en un *Trading Desk* es un *Media Trader*.
Los *Trading Desks* pueden integrarse en una agencia de medios, ser completamente independientes y haber sido creados ex-nihilo o incluso estar montados internamente por grandes anunciantes.

RTB*:

RTB son las siglas que se utilizan normalmente en el campo de la publicidad en internet y probablemente cada vez más en el campo de los medios «tradicionales» para referirse al concepto de pujas en tiempo real o «*Real Time Bidding*».
En el marco del RTB *display*, una impresión publicitaria se subasta en tiempo real en un marketplace (*Ad Exchanges*, plataforma programática, etc.) cuando un usuario consulta una página o se mete en una app. Salvo excepciones y acuerdos especiales, es entonces cuando el anunciante que ha hecho la oferta ve difundida su creatividad. Dependiendo del caso, la subasta puede haber sido preestablecida o determinada en una décima de segundo por un algoritmo de pre-puja.
El RTB se asocia inicialmente a compras programáticas por internet, pero no todas las compras programáticas se realizan en RTB. El uso de RTB en el proceso de compra de espacios de publicidad digital está en constante aumento y ya no está reservado como al principio para espacios de calidad más baja.

Programática garantizada:

La programática garantizada es un modo de compra de espacio publicitario automatizado (programático) mediante el cual el espacio publicitario vendido no se subasta en RTB, sino que se vende previamente a un anunciante a través de un «*private deal*». También hablamos de programática directa.

El término programática directa se utiliza principalmente en el contexto de la venta de espacios digitales, en el cual una buena parte se hace ahora en modo programático. Sin embargo, el uso del término también puede aplicarse a los medios tradicionales, que también se ven vencidos por los modos de gestión programática.

Yield Management:

En el ámbito de la monetización de la publicidad, el *Yield Management* es la práctica de optimizar los ingresos publicitarios mediante la adopción de un método de fijación de precios más o menos dinámico que se adapte a la demanda de agencias y anunciantes.

El *Yield Management* practicado por una agencia de publicidad puede afectar a la mayoría de los medios. Es en el campo de la publicidad digital que el proceso puede ser más exitoso ya que en plataformas programáticas el ajuste de la tarifa se puede hacer en tiempo real e impresión por impresión en función de las subastas de los anunciantes (RTB). Cuando esta optimización de los ingresos se hace englobando a la vez los métodos de comercialización directos y la venta en RTB, se denomina proceso de *yield* holístico.

En los medios tradicionales, la noción de *Yield Management* a menudo se ajusta a la creación de tarifas específicas para reservas de última hora o para horas valle. Sin embargo, la digitalización de los medios tradicionales (televisión programática, DOOH programático, etc.) debería desarrollar gradualmente el uso de un *Yield Management* más dinámico y automatizado y la noción de *Yield Management* holístico también podría concernir a dichos medios.

Ad Server full-stack:

Un *Ad Server* full-stack es un término que a veces se utiliza para describir una plataforma que administra tanto las funciones de comercialización en RTB como las funciones clásicas de *Ad Trafficking* de un servidor de anuncios.

El *Ad Server full-stack* va mucho más allá de un «simple» *Ad Server*.

Es una solución técnica para la gestión y monetización de espacios publicitarios que combina el *Traffic Management*, los procedimientos de comercialización en RTB y los modos clásicos o históricos de comercialización (venta directa, operaciones especiales, etc.).

Una plataforma full-stack debería teóricamente permitir eliminar la superposición de diferentes soluciones técnicas (*Ad Server* - SSP – *Ad Exchange*) y optimizar la monetización a través de un proceso llamado *yield* holístico.

Blind Network:

Una *Blind Network* es una red de publicidad en la cual los anunciantes compran espacio publicitario sin saber qué sitios mostrarán sus anuncios.

La compra se hace a ciegas porque la red se compone tanto de un gran número de sitios con inventarios limitados, como de sitios importantes que no quieren que los anunciantes sepan que están «liquidando» sus anuncios no vendidos que por lo general se venden a CPM «superiores».

Incluso si los sitios de soporte utilizados no se comunican a los anunciantes, las *Blind Networks* pueden ofrecer opciones de *targeting* temático.

Las *Blind Networks* suelen comercializar espacios para los anunciantes a un rendimiento o CPM muy bajo.

Header Bidding:

El *Header Bidding* es un proceso interno de gestión de publicitaria que permite a los editores subastar impresiones de publicidad digital a un mayor número de *Ad Exchanges*, SSP o *Trading Desks* y poner a competir a estos compradores potenciales por la vía habitual/interna de comercialización. El término *Header Bidding* se utiliza porque el proceso se realiza insertando uno o más códigos específicos (*tags*) en el *header* de la página que hospeda la creatividad.

DMP:

DMP son las siglas de *Data Management Platform* (plataforma de gestión de datos). Es una plataforma que normalmente se ofrece en modo SaaS y que permite recopilar, centralizar, administrar y utilizar los datos de clientes potenciales.

Las primeras DMP se centraron en los datos de navegación, que se utilizaron con fines de publicidad comportamental. Ahora, las DMP más avanzadas integran los diferentes puntos de contacto para la recopilación de datos y el *targeting* y combinan el *offline* y el *online* utilizando métodos de *CRM onboarding*.

Los datos gestionados por una DMP también se pueden enriquecer con datos de «especialistas en datos» de terceros.

Los datos gestionados por DMP se utilizan para optimizar el *targeting* y la eficacia de las campañas de marketing y de publicidad con una posible finalidad de personalización en sitios y apps. La DMP puede ser vista como la heredera de la «tradicional» base de datos de clientes y se ha convertido en un pilar del CRM a través de la implementación de un repositorio único de los datos del cliente.

Las DMP ofrecen muchos tipos de servicios o características a las empresas que lo utilizan, algunas de los cuales hacen la gestión de potenciales clientes y audiencias publicitarias en una lógica de PRM (*Prospect Relationship Management*). Una parte del ROI relacionada con la implementación de una DMP puede lograrse potencialmente a través de la activación de datos.

Algunos ejemplos de las funciones de una DMP:

- Análisis y calificación de audiencia
- Servicios de *data exchange*
- Ventas de datos a sitios o redes de terceros
- Uso de datos para el *targeting* multicanal
- Servicios de extensión de audiencia
- Herramientas de protección de datos
- Medición del ROPO (*Research Online Purchase Offline*)
- Medición del ROI offline de las inversiones digitales

First Party Data:

Los *First Party Data* se refieren a los datos susceptibles de *targeting* que recopila directamente el sitio del editor. Los datos de primera parte suelen ser datos comportamentales o declarativos registrados en el sitio de soporte durante visitas anteriores y que están asociados a los visitantes gracias a una *cookie*.

El término *First Party Data* luego se expandió a todos los actores de internet y por lo tanto se refiere a todos los datos disponibles para una empresa o anunciante propietario de estos. El concepto de datos de primera parte designaba originalmente los datos recopilados *online*, pero también abarca ahora datos CRM / *offline*, especialmente cuando estos se reconcilian con los datos de internet dentro de una DMP por un procedimiento de *CRM onboarding*.

Third Party Data:

Los *Third Party Data* suelen ser datos de *targeting* publicitario que se hacen llegar al anunciante por una compañía de terceros que no sea el editor usado como sitio de soporte para una campaña.
Los datos de tercera parte son proporcionados principalmente por agencias de publicidad, especialistas en datos o procedimientos de *data exchange* en *data marketplaces*. Estos datos comportamentales o declarativos se recopilan y se asocian a los visitantes gracias a *cookies*.
En un comercio *online*, los datos de tercera parte se pueden utilizar para personalizar la oferta, a pesar de que sea la primera vez que el usuario visita el sitio.
El concepto de *Third Party Data* se ha popularizado por los usos del marketing digital, pero los datos externos también pueden tener un origen *offline* (datos sacados de *partners*, datos de enriquecimiento B2B, etc.).

CRM onboarding:

El *CRM onboarding* es la práctica mediante la cual se utilizan los datos *offline* de un CRM para poder encontrar y llegar a una parte de los clientes en el entorno internet/digital.
En el marco de un proceso de *CRM onboarding*, la base de clientes/CRM de una empresa se sube a una plataforma de *onboarding* y los registros se comparan (*matching*) con las bases de datos de individuos identificados por una *cookie* o identificador móvil. Las personas que coincidan en la base CRM de la empresa y en las bases utilizadas por la plataforma de *onboarding* ahora podrán ser *target* de la empresa en el entorno digital a través de una *cookie* u otro tipo de identificador digital. Se trata de «digitalizar» los datos puramente *offline* del CRM.
El *CRM onboarding* permite a las empresas encontrar, reconocer y dirigirse a sus clientes en la red sin que necesariamente hayan utilizado o visitado un sitio web de dichas empresas o cuando la *cookie* ya no está funcionando. Esta práctica también permite reconocer en el sitio del anunciante a clientes que jamás se han identificado o *logueado*.
En el marco de un proceso de *CRM onboarding*, no todos los clientes o posibles clientes presentes en la base de datos pueden ser encontrados y se les asigna un identificador digital. Se considera normalmente que la tasa de conciliación está entre un 30% y un 50%.

DCO:

DCO son las siglas de *Dynamic Creative Optimization*. Por lo tanto, el DCO es la práctica mediante la cual las creaciones de publicidad digital (*banners*, anuncios de Facebook, vídeos, etc.) se optimizan automáticamente en tiempo real a medida que se difunden. El DCO tiene el objetivo de maximizar la tasa de clics y / o la tasa de conversión en el sitio del anunciante.

El primer nivel de DCO que se llamará aquí «DCO simple» consiste «simplemente» en adaptar en tiempo real la creación de publicidad en función de los elementos de contexto relacionados con el individuo *targetizado* (datos individuales, ubicación, etc.) o el contexto del entorno (hora, clima, etc.). Se pueden hacer muchas creaciones e incluso pueden ser únicas en el caso por ejemplo de la distancia a un punto de venta que se muestre en el mensaje.

*source : www.definitions-marketing.com

En resumen, para detectar el grado de fraude del cual el anunciante es potencialmente víctima, este último dispone de dos enfoques emparejados que permiten evaluar la calidad de sus inversiones digitales:

Un enfoque puramente cuantitativo de análisis y de cruce de los datos disponibles en las herramientas de análisis y de atribución, los servidores de publicidad (*Ad Server*), las plataformas de subastas de publicidad, así como las herramientas de gestión de compra programática (DSP) para detectar métricas que no correspondan a valores esperados o que haya variaciones inconsistentes. Un enfoque más cualitativo de análisis de los procesos de implementación de la campaña por parte del anunciante y sus agencias (*briefing*, *reporting*, elección de KPIs [indicadores clave de rendimiento], objetivos, *targets*, etc.) con el fin de contextualizar y comprender los datos analizados.

En cuanto a las recomendaciones que poner en marcha, las principales acciones son:

1) Internalizar el acceso y almacenamiento de datos para conservarlos y analizarlos.

2) Definir procesos de gestión del fraude en el anunciante (equipo directivo, marketing, digital...) y en la agencia (informes, selección de editores, listas negras de sitios, ...).

3) Tener expertos internos que puedan verificar la coherencia del rendimiento y analizarlo en detalle.

4) Incorporar herramientas tecnológicas de análisis del mix de medios del tráfico, siempre estando atento a la relación entre el rendimiento y el coste.

Para cada recomendación propuesta, es importante evaluar los medios y recursos que se utilizarán (internos o externos, herramientas, procesos, etc.) gracias a un análisis de la relación entre los costes totales y los impactos con el fin de priorizar las acciones que tomar. Es importante subrayar que estas acciones no reducirán el fraude a cero, lo cual es un objetivo inalcanzable, sino que más bien limitarán el fraude y limitarán su volumen.

Es paradójico pensar que la proporción de fraude es mayor en la publicidad digital que en la publicidad tradicional, cuando la promesa de la publicidad digital es la transparencia total de las inversiones en medios: la identificación de la publicidad utilizada, el sitio de difusión, el usuario *targetizado* (a través de *cookies*), su visibilidad y la medición de la conversión de cada anuncio adquirido.

De hecho, es la granularidad infinita y la complejidad asociada a la compra de espacios en internet lo que abre un abanico de oportunidades para los estafadores. Esta granularidad es lo que da fuerza a la publicidad digital, pero a la vez lo que dificulta el control de todos los anuncios comprados y la conformidad con los pedidos del anunciante. Existen herramientas de control y medición para limitar el fraude de la publicidad digital, pero por sí solas no serán suficientes. El éxito depende de la cooperación del conjunto de los actores del sector: anunciantes, agencias, vendedores de espacios y proveedores de soluciones tecnológicas. Es importante tomar el toro por los cuernos con el tema del fraude de cara al futuro del ecosistema digital y para preservar la confianza de los actores.

1A EDICIÓN

Libro Blanco - Fraude, el lado oscuro del Marketing Digital
Fecha de publicación: septiembre 2017
Adaptación al español: marzo 2020

Contacto:
Collectif de la Performance & de l'Acquisition
8 rue Saint Fiacre
75002 París – Francia

T. (33) 01 77 45 46 23
E. contact@cpa-france.org
www.cpa-france.org
Twitter: @CPA_Performance

Noella Boullay: Delegada General - nboullay@cpa-france.org
Joy Grand: Responsable de Comunicación - jgrand@cpa-france.org

AGRADECIMIENTOS

Un agradecimiento muy especial para Joy Grand

Diseño gráfico:
Flavie Ferrari
www.flavieferrari.com
06 51 02 70 70

Un agradecimiento particular por la relectura para:

Gregory Bocquenet
Chief Sales Officer
CibleClic SAS

Julien Dugaret
CEO
Beyable

Rahim Daouadji
Business Developer
Chameleon Ad

Timothée Le Roy
Responsable de Marketing y Comunicación – Matlo

Oualid Barbouchi
CEO and Co-founder
PRM Factory

A los miembros del Consejo de Administración del CPA:

SOBRE EL CPA:

Creado en 2008, el CPA (Colectivo para los Actores del Marketing Digital) es el sindicato profesional de los actores del marketing digital de performance, un sector de actividad que constituye la base de toda estrategia de adquisición digital.

El CPA representa a editores y proveedores expertos, ofreciendo soluciones independientes y personalizadas a los decision makers del marketing digital (anunciantes y vendedores online) para apoyar su desarrollo. A través de sus acciones (Libros Blancos, Cartas de calidad, recomendaciones, eventos y Networking), el CPA cumple cuatro objetivos principales:

- Regular un mercado en crecimiento y en constante cambio,
- Informar sobre las mejores prácticas de adquisición digital,
- Garantizar su puesta en marcha en la aplicación del marco legal,
- Representar los derechos e intereses de sus miembros.

Ante la proliferación de modelos de adquisición y Customer Journeys cada vez más complejos, los miembros del CPA se comprometen a poner su expertise, comprensión del sector y espíritu innovador al servicio de sus clientes. El CPA une a los principales actores del mercado del marketing digital de performance con 10000 puestos de trabajo y una facturación de 2300 millones de euros.