FRAUDE

Le côté obscur du Marketing Digital

Édition 2017

AVEC NOS REMERCIEMENTS POUR LA PARTICIPATION :

Didier Beauclair
Directeur Stratégies & Médias
UDA

Grace Paynot
Responsable Marketing Digital, CRM et Communication
PSA BANQUE

Thomas Hadjadj
Digital Acquisition Marketing Manager Head of display Europe
MEETIC

Paulo Esteves
Head of Marketing
SELENCY

Alexandre Schont
Responsable Business Development
TABMO

Fabien Omont
Responsable Data & Attribution
OATH

Jeremy Giacomini
Chief Digital Officer
FONCIA

PUBLICATION : SEPTEMBRE 2017
Travaux menés par les membres du Collège Technologies
E-marketing du Collectif de la Performance & de l'Acquisition :

CO-RÉDACTEURS

Christophe Bosquet
Co-founder & CEO
effinity

Emmanuel Brunet
CEO
EULERIAN TECHNOLOGIES

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
Déléguée Générale

Joy Grand
Chargée de Communication

SOMMAIRE

PRÉFACE

Les investissements des annonceurs dans la publicité digitale ne cessent de progresser. En France, ils étaient de l'ordre de 3,5 milliards d'euros en 2016 (source #Obsepub) quand, à l'échelle mondiale, ce chiffre est estimé à environ 130 milliards d'euros (source WFA).

En même temps que les investissements progressent, les chemins qu'ils empruntent se complexifient. Les chaînes d'intermédiation s'allongent, les prestataires techniques se multiplient. La distance entre les éditeurs et les producteurs de contenus ne cesse de s'agrandir, au détriment de la véritable traçabilité des sommes en jeu. Fort légitimement, les annonceurs sont préoccupés de performance et de retour sur investissement et sur ce plan, l'Internet publicitaire se fait fort de fournir des preuves et une quantification de son efficacité (au risque d'ailleurs pour les annonceurs de se tromper d'indicateur et de prendre des vessies pour des lanternes !). Taille du marché, complexité des structures, obsession du résultat : dans cet immense creuset mondial de la publicité digitale, tous les ingrédients sont donc réunis pour que s'épanouisse une fraude à grande échelle qui se joue des frontières.

D'ores et déjà un grand nombre d'annonceurs ont pris conscience de la nécessité de s'armer contre la fraude digitale mais l'hydre de Lerne, avec ses sept têtes, ferait pâle figure devant la multiplicité des formes qu'elle peut revêtir ! En 2016, l'UDA a participé à l'élaboration du guide «Compendium of ad fraud knowledge for media investors» publié par la WFA (Fédération mondiale des annonceurs) qui dressait un premier inventaire de la fraude et estimait même qu'à l'horizon 2025, elle pourrait représenter entre 10 et 30 % du marché total de la publicité digitale. Opérée par des black hat marketers, voire par ceux que la WFA nomme pudiquement organised criminals, la fraude digitale dépasse bel et bien les seuls enjeux du marché publicitaire.

Devant l'ampleur du phénomène et des risques qu'il fait courir non seulement à notre économie mais aussi à notre société, il est essentiel que tous ensemble - plateformes, annonceurs, agences, éditeurs...

Nous nous mobilisions pour faire reculer la fraude. Dans ce combat commun, la première des actions à entreprendre est celle de l'information et de la sensibilisation de tous et c'est l'enjeu du présent document. En dressant une liste la plus exhaustive possible des différentes formes que revêt (à ce jour !) la fraude digitale, il permet à chacun d'être désormais vigilant et de mettre en place, chaque fois que possible, des mesures de protection.

Parallèlement à sa mobilisation contre la fraude, les actions de l'UDA et de ses partenaires en faveur de l'amélioration de la qualité de l'Internet publicitaire sont multiples. On peut en particulier citer :

• Le label Digital Ad Trust. Lancé en France à l'automne 2017 par les annonceurs, les agences médias, les régies de l'Internet et les éditeurs, il permet aux sites qui en remplissent les critères d'obtention, d'être labellisés DAT.

Les critères portent sur cinq grands chapitres : le contrôle de la fraude, la qualité de l'expérience utilisateur, le respect des données personnelles, la visibilité de la publicité et la protection des marques.

• La Coalition for better ads. Initiative internationale, la «coalition» notamment portée par la WFA, a d'ores et déjà publié une liste de formats considérés comme intrusifs et directement de nature à favoriser la pénétration des bloqueurs de publicité auprès des internautes.

• L'European viewability certification framework. Issu d'une collaboration interprofessionnelle européenne, cette initiative crée le cadre d'une certification des outils de mesure de la visibilité de la publicité digitale.

Créer ensemble un marché de la publicité digitale transparent, contrôlé, mesuré et respectueux de l'internaute, tant au niveau national, qu'européen et mondial, c'est tout l'enjeu de l'action de l'UDA et de ses partenaires pour restaurer la confiance.

Cette initiative du CPA y participe directement et nous nous en réjouissons.

Didier Beauclair
Directeur Stratégies & Médias
Union des annonceurs
UDA

PRÉFACE

Posons la première pierre…

La fraude est le propre de l'homme ! Elle est, en effet, présente dans toutes les activités humaines. Le sport, la politique, les jeux de hasard, la finance, le monde des affaires, etc. Partout où il existe des règles et un gain potentiel, il existe des personnes ou des organisations qui tentent de contourner ces règles à leur avantage pour s'attribuer une part des gains. Si tricher, n'est pas jouer, frauder, c'est souvent gagner !

Alors faut-il s'étonner, que le digital, un univers en pleine croissance, qui attire de plus en plus d'annonceurs et d'investissements, soit, lui-aussi, victime des fraudeurs ? Assurément pas. La fraude est le revers de la médaille du succès !

Il semble aussi important de rappeler que le contexte général du monde des affaires n'est pas sans influence sur la fraude. La culture du résultat (au détriment de l'analyse des moyens), la pression permanente pour faire baisser les tarifs (on ne touche pas les femmes enceintes de Grenoble à un euro du CPM), la déshumanisation des relations, etc. sont autant d'incitations qui favorisent la fraude. A l'évidence, aucun secteur d'activité n'a réussi à éliminer complètement et définitivement la fraude. Dès que l'on ferme une brèche, une autre s'ouvre. Et le digital n'y parviendra pas non plus.

Cela dit, il est indispensable de combattre la fraude fermement, pour la faire diminuer, bien sûr, mais aussi pour « sauver l'honneur » de la profession. Tous les sportifs ne sont pas dopés, tous les politiques ne sont pas « pourris », tous les acteurs du digital ne sont pas des fraudeurs !

C'est un travail quotidien et chacun dans la chaîne du digital (annonceurs, agences, éditeurs, prestataires divers, etc.) doit s'y atteler en se remettant en question, en analysant ses pratiques, etc. Souvent, la fraude naît de règles imprécises qui laissent une marge de manœuvre aux fraudeurs : un contrat qui ne précise pas suffisamment les livrables, une organisation qui ne différencie pas ceux qui contrôlent de ceux qui achètent, etc. Cela permettra, si ce n'est d'éliminer la fraude, en tous cas de la différencier des mauvaises pratiques. Et il est absolument nécessaire de réaliser cette différenciation, pour que l'essentiel de nos efforts pour lutter contre la fraude se dirigent vers les bonnes cibles.

C'est la raison pour laquelle le CPA a choisi de dédier ce livre blanc exclusivement aux techniques de fraude. Pour que chacun puisse clairement identifier les zones de faiblesse à surveiller. Comme vous pourrez le lire, des solutions existent pour limiter la fraude. Elles sont souvent issues du bon sens et pas si compliquées à mettre en place.

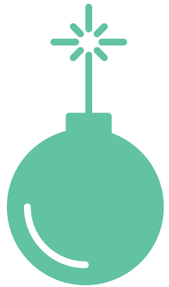
À l'heure où tous (médias, annonceurs, etc.) semblent découvrir et s'étonner que la fraude existe dans le digital, il nous a paru important d'apporter des éléments tangibles et rationnels sur le sujet. L'enquête que nous avons menée auprès des annonceurs et agences sur la fraude dans le Display va dans ce sens.

Nous souhaitons donc que ce livre blanc vous permette de comprendre les systèmes de fraude pour vous en prémunir au mieux dans votre activité. Ce n'est certes pas la construction d'un mur hermétique à la fraude, mais une pierre fondatrice qu'il nous a semblé nécessaire de poser.

Christophe Bosquet
Président du Collège Technologies Marketing du CPA
effinity

ÉDITO

LA FRAUDE EN MATIÈRE DE PUBLICITÉ DIGITALE SERAIT AUJOURD'HUI L'ACTIVITÉ ILLÉGALE LA PLUS LUCRATIVE DU MONDE APRÈS LA DROGUE. QUAND ON PARLE DE FRAUDE EN MATIÈRE DE DIGITAL, LA RÉACTION UNANIME EST DE PENSER AUX PROBLÈMES DE SÉCURITÉ INFORMATIQUE ET DE FALSIFICATION DE DONNÉES PERSONNELLES ET FINANCIÈRES.



Il existe pourtant une fraude digitale moins connue, mais dont l'impact financier est bien supérieur : la fraude en matière de publicité digitale.

La World Federation of Advertisers estime que l'impact pourrait être de l'ordre de 30 à 40% des investissements médias digitaux mondiaux en 2025, soit un montant de l'ordre de 150 milliards de dollars.

Sans attendre 2025, White Ops, firme de cyber-sécurité américaine spécialisée dans la fraude publicitaire a révélé en décembre 2016 l'existence d'un vaste système d'escroquerie monté par des hackers russes. En créant de faux sites, alimentés par un faux trafic, le réseau Methbot génèrerait jusqu'à cinq millions de dollars par jour.
Concrètement, l'escroquerie fonctionne de la manière suivante :
Le réseau Methbot a pris le contrôle de plus de 500 millions d'adresses IP.
À chacune de ces adresses IP, les hackers ont également attribué des bots, des programmes conçus pour imiter les habitudes de navigation d'un humain (démarrage de vidéo, chargement de pages).

En parallèle, les opérateurs russes se sont fait passer pour 6 000 sites de premier plan : des médias tels que CNN et Fox News, des réseaux sociaux comme Facebook ou encore des sites de marques comme Pokémon.
Les annonceurs ont ensuite été piégés en achetant de l'espace sur ces sites via des ad-exchanges à des CPM élevés variant de $3 à $37.
Certains annonceurs ont bien compris l'impact financier de la fraude digitale et sont en train d'agir pour y faire face.
Au sujet de la fraude, viennent s'ajouter, dans les chiffres donnés par la presse, les sujets de transparence et de mesure.
Premier annonceur mondial, Procter & Gamble a demandé à ses agences, en février 2017, de faire un effort de transparence sur les tricheries qui faussent les chiffres de la publicité en ligne. P&G a annoncé 5 mesures pour lutter contre l'opacité dont l'adoption d'une unique norme de visibilité développée par le Media Rating Council et l'utilisation de la certification Trustworthy Accountability Group pour prévenir les pratiques malveillantes et/ou illégales.

DANS LE MÊME TEMPS, LE DÉCRET D'APPLICATION DE LA LOI SAPIN À LA PUBLICITÉ DIGITALE A ÉTÉ FINALEMENT ADOPTÉ AU JOURNAL OFFICIEL DU 9 FÉVRIER 2017.

LA LOI SAPIN

La volonté de la publication de ce texte de loi avait redoublé suite à la révélation en juin 2016 des pratiques d'agences média aux Etats-Unis qui avait provoqué un scandale, et le débat était régulièrement relancé par les découvertes de fraudes publicitaires de grande ampleur à l'instar de White Ops fin décembre 2016 (qui a découvert Methbot).

Ce décret confirme l'application à la publicité en ligne des grands principes de transparence de la loi Sapin de 1993 sur les transactions publicitaires opérées sur les médias. Certaines obligations sont demandées aux vendeurs d'espaces :

L'article 2 dudit décret prévoit les mentions à porter sur le compte rendu communiqué par le vendeur d'espaces publicitaires à l'annonceur :

« La date et les emplacements de diffusion des annonces, le prix global de la campagne ainsi que le prix unitaire des espaces publicitaires facturés ».
L'article 3 encadre le processus automatisé d'achat d'espaces publicitaires sur Internet afin d'agir contre la fraude au clic publicitaire résultant de l'utilisation de robots destinés à fausser les données de trafic. Le vendeur devra désormais communiquer à l'annonceur un compte rendu comportant : « les informations qui permettent de s'assurer de l'exécution effective des prestations et de leurs caractéristiques ; les informations qui permettent de s'assurer de la qualité technique des prestations ; les informations sur les moyens mis en œuvre pour protéger l'image de la marque de l'annonceur »

ACTEURS LEADERS DU MARCHÉ, FACEBOOK ET GOOGLE SONT SOUPÇONNÉS DE NE PAS RENDRE TRANSPARENTES LES MESURES D'AUDIENCE. LES PERFORMANCES DES PUBLICITÉS DIFFUSÉES SUR GOOGLE ET FACEBOOK SONT AUTO-MESURÉES : IL N'Y A PAS DE TIERS DE CONFIANCE.

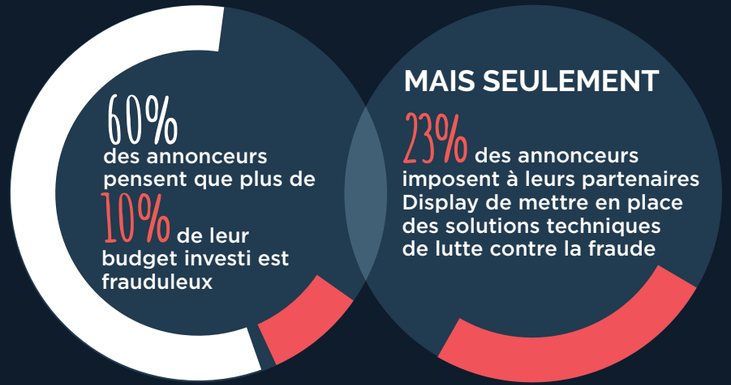
Google

En 2015, des chercheurs européens ont menés une expérience qumontre que YouTube (i.e. Google) a facturé les annonceurs même lorsque leurs publicités étaient vues par des robots plutôt que des êtres humains.
Cela a eu lieu alors que YouTube était tout à fait capable de les identifier comme des robots.
Des questions ont alors été posées sur les intérêts de YouTube à faire gonfler artificiellement l'audience, puisque son modèle économique est directement lié au trafic généré.

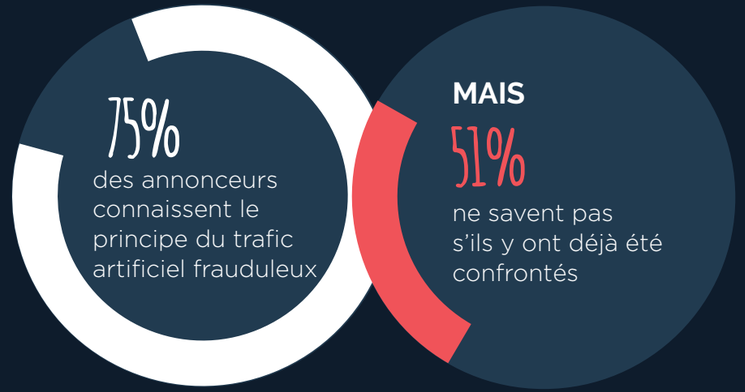
Critiqué pour de nombreuses erreurs commises dans la mesure de ses audiences, le réseau social a joué l'apaisement en s'ouvrant à des mesureurs tiers.
La plateforme a été épinglée à plusieurs reprises depuis l'été 2016 pour des erreurs dans les mesures d'audience qu'elle communique aux agences et annonceurs qui achètent du media chez le réseau social.
Facebook a alors permis aux annonceurs de vérifier la visibilité des impressions display grâce à des partenaires tiers comme MOAT, IAS et Comscore.
Cependant, ces nouveaux partenaires ne taguent pas les pages Facebook comme ils le font sur les sites. En temps normal, le mesureur pose son tag javascript autour de la publicité. Celui-ci mesure alors toutes les 100 millisecondes si la bannière est visible et dans quelles proportions. Mais pas sur Facebook. Le mesureur se contente de retraiter et analyser des données brutes qui sont remontées par Facebook

Dans le cadre de son Livre Blanc, le CPA a mené une étude à l'aide d'un questionnaire sur l'état de la Fraude en Display adressé aux annonceurs et agences, auquel nous avons obtenu le retour d'une centaine de répondants.
Le traitement de ces réponses a permis d'établir quelques constats :

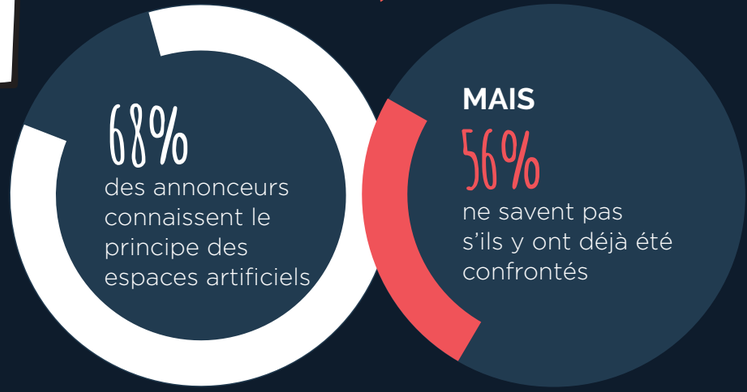
CONSTAT



LE TRAFIC ARTIFICIEL



LES ESPACES ARTIFICIELS



PARTIE 1. VENDRE UN ESPACE FICTIF

INTRODUCTION

La fraude en matière de publicité digitale se décompose en quatre grands thèmes :

1) Les faux espaces

> Plus de 40% des publicités facturées et diffusées sur Internet ne sont effectivement pas vues par les visiteurs, soit parce qu'elles sont placées sous la ligne de flottaison, soit parce que ce ne sont pas des humains qui sont exposés à cet espace.

2) Le faux trafic

> Les robots seraient responsables de 6% à 9% du trafic comptabilisé en 2015.

3) Le mauvais ciblage

> Certains ciblages annoncés, sur la base de critères sociodémographiques ou d'intérêts personnels (âge, géographie, sexe, profession, hobbies...), ne correspondent pas à la réalité des internautes réellement exposés à la campagne publicitaire.

4) Les rendements biaisés

> Certains éditeurs manipulent la navigation des internautes pour augmenter leurs rendements.

Les espaces artificiels sont des espaces publicitaires fantômes destinés à 'tromper' les outils d'Ad-Serving en leur faisant croire que la publicité est affichée correctement

- comme sur un site 'vertueux' - alors qu'elle n'est soit pas diffusée, soit diffusée de telle manière qu'elle devient ineffective, soit diffusée auprès de robots. En bref, il s'agit de modalités techniques qui détournent les publicités de leur objet d'information pour ne conserver que la génération de revenus pour le fraudeur.

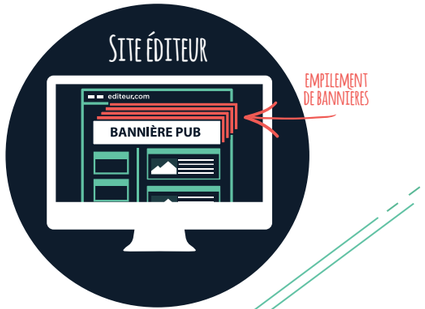
ON PEUT RECENSER 6 CATÉGORIES D'ESPACES FICTIFS :

1. LE PIXEL STUFFING

Le fraudeur réduit les publicités à un simple pixel (taille 1x1 - invisible) qui appelle l'Ad-Server sans afficher la publicité correspondante. Toutes les fonctions attachées à l'Ad Server restent actives : une impression est comptée, un cookie est déposé mais l'utilisateur n'a rien vu. Cette technique permet d'afficher des dizaines de publicités sur une seule page générant d'importants volumes d'impressions même sur un site à faible trafic.

2. L'EMPILEMENT DE PUBLICITÉS OU AD STACKING

Sur un seul emplacement publicitaire, le fraudeur empile des publicités les unes sur les autres, une sorte de mille-feuille digital. Chaque Ad Server impliqué considère que les publicités sont affichées et facture les annonceurs pour cette diffusion, le dépôt de cookie s'effectue bien alors que seule la bannière du dessus est visible par l'internaute. Comme dans la catégorie précédente, on peut afficher et s'assurer les revenus de multiples publicités dans un minimum d'espace.
Dans le même registre, le fraudeur peut cacher des bannières derrière un habillage publicitaire. Seul l'habillage sera visible pour l'internaute.



3. LES SITES FANTÔMES

Il existe des sites fantômes qui ressemblent à des sites légitimes mais sont truffés de publicités et visités quasi-exclusivement par des robots. Le détenteur du site – le botmaster – s'inscrit comme un diffuseur légitime auprès de réseaux d'affiliation ou de SSP, il passe les phases de contrôle de ces prestataires car le site existe vraiment et semble actif même si le contenu est bien souvent copié depuis des blogs ou des encyclopédies comme Wikipedia. Une fois référencé comme diffuseur, le site va afficher des publicités depuis différents prestataires mais celles-ci ne seront pas vues par des humains mais plutôt par des robots.

4. L'AUTO-REFRESH

Cette méthode consiste à rafraîchir automatiquement un même emplacement publicitaire avec une publicité différente à chaque rafraîchissement.
Les publicités sont donc toutes visibles par l'internaute mais pour un temps très court.

5. LES MALWARES SUR MOBILE (MOBILE DEVICE HIJACKING)

Des applications, pourtant validées dans les appstores s'exécutent en tâche de fond et réalisent des affichages et des clics, même si l'application est fermée ou n'a jamais été ouverte ! Elles peuvent s'exécuter au démarrage de l'appareil, à la mise en veille, au verrouillage d'écran etc. Les publicités sont invisibles par l'utilisateur mais les faux clics et affichages générés par ces applications peuvent concerner de gros volumes. Ces applications établiraient jusqu'à 1100 connexions par minute et communiqueraient avec 320 réseaux publicitaires.

> Le risque de fraude 0 n'existe pas et peut venir à la fois de l'éditeur final comme des intermédiaires.
> Maîtriser la chaîne de valeur en réduisant le nombre d'intermédiaires est un prérequis.
> En complément, il est primordial d'ajouter des outils de contrôle indépendants ainsi que d'évaluer précisément la contribution réelle des canaux marketing sur les ventes finales.

Fabien Omont
Responsable Data & Attribution
Oath:

6. LES PUBLICITÉS CACHÉES DANS DES APPLICATIONS MOBILES

Comme sur une page Web, il existe des cas de fraude d'empilement de publicités ou de bannières invisibles dans une application.
Ces publicités sont appelées directement dans le code de l'application sans être affichées, elles ne sont pas visibles pour l'internaute.

PARTIE 2. VENDRE UNE AUDIENCE FICTIVE

INTRODUCTION

Une partie importante de la fraude publicitaire sur Internet se fait par le biais de robots. Ils peuvent être plus ou moins sophistiqués et ne sont pas tous malveillants. Certains robots servent Internet de manière positive, par exemple pour améliorer les moteurs de recherche. Ceux-ci se déclarent auprès des technologies de collecte de données afin de ne pas être comptabilisés dans les différents reportings, notamment grâce au fichier «robots.txt».

Les robots malveillants, par contre, ont pour objectif de créer de l'audience fictive et de simuler le comportement humain afin de générer des visites sur des sites, des impressions ou des clics sur des publicités. C'est l'activité de pirates, souvent organisés en réseau, qui usurpent les adresses IP d'ordinateurs afin de simuler des actions publicitaires pour lesquelles ils récoltent les revenus.

Comme dans un remake de Terminator version ad tech, le robot est le cauchemar de l'acheteur média. Il n'a pas de cœur, pas de cerveau et surtout aucun moyen de paiement susceptible de l'amener sur la page de finalisation de commande chez un e-commerçant. Et pourtant, le robot est partout. Et pas toujours inutile.

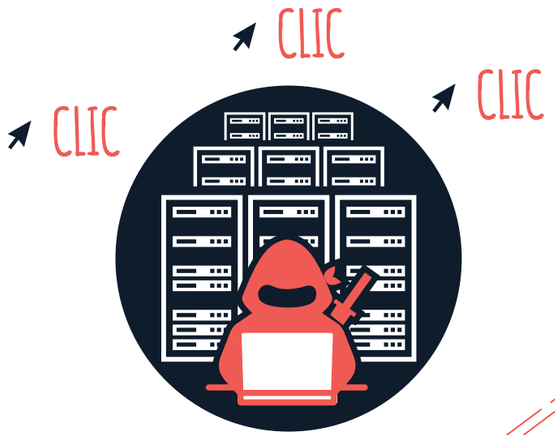
Selon une étude Imperva de 2016*, les «mauvais» robots représentent 28,9% du trafic Internet .

*http://robots-txt.com/

ON DISTINGUE 3 TYPES DE BOTS FRAUDULEUX, DU PLUS SIMPLE AU PLUS SOPHISTIQUÉ :

1. LE BOT INDÉPENDANT

Ce type de robot a pour objectif de simuler des impressions et des clics sur des publicités à partir d'un ordinateur simple. Les pirates qui développent ce type de bot se concentrent sur les acteurs qui ne considèrent pas la fraude comme une menace et qui n'ont pas mis en place d'outils de détection spécifiques. S'ils font attention de ne pas générer des revenus trop importants, leur activité peut durer un petit moment.
Certains robots sont capables d'imiter des comportements humains, comme le mouvement de la souris, la navigation sur une page Web, des visites sur des pages, des clics sur différents liens, le lancement de vidéos ... Ils sont beaucoup plus difficiles à identifier que les autres robots.



2. LE BOT DATA CENTER

Celui-ci est plus complexe et ne peut être opéré que par une organisation ayant accès à plusieurs serveurs afin de multiplier les adresses IP. Ces bots reproduisent les actions des bots autonomes mais de manière massive.

Les datacenters permettent de louer des ordinateurs à la durée, il est donc possible de les utiliser pour une courte période pour lancer les bots.

3. BOTNET : LE RÉSEAU DE BOTS MALWARE

Le malware, ou programme malveillant en français, est un virus installé sur un ordinateur. L'intérêt pour le fraudeur, outre le fait qu'il a la main complète sur l'activité en ligne de l'internaute, c'est qu'il peut analyser son comportement et le cloner, de manière à générer des comportements qui parviennent à tromper les outils anti-fraude.
Les bots malware sont programmés pour se connecter au réseau de machines Botnet pour lancer des tâches en parallèle en se faisant passer pour un véritable internaute.

Nous distinguons deux types de fraude : la fraude à l'impression et la fraude au clic. Foncia travaille dans le temps avec des acteurs de confiance, il y a très peu de cas de fraude. Lorsqu'on intègre un nouveau partenaire, il y a une phase de tests, si les résultats ne sont pas là, nous le mesurons tout de suite.

Jérémy GIACOMINI
Chief digital officier

LES « FERMES À CLICS »

En juin 2017, une filière a été démantelée par les autorités Thaïlandaises après la découverte d'une «ferme à clics» composée de 500 téléphones mobiles, utilisant 400 000 cartes SIM différentes

(source : 01Net - 13/06/2017: http://www.01net.com/actualites/cette-ferme-a-clicsfonctionnait-grace-a-500-iphone-et-400-000-cartes-sim-1185520.html).

Ce type de dispositif est surtout utilisé pour générer des «Likes» sur les réseaux sociaux. Mais on peut imaginer de telles installations dans le but de générer des faux clics sur des publicités. A noter que les faits reprochés aux personnes impliquées dans cette affaire sont liés à l'absence de permis de travail et non pas à la nature de leurs activités.

4. L'IFRAME STUFFING

Au-delà des bots, il existe une méthode simple de génération de trafic fictif pour un webmaster en appelant une page Web voire un site entier dans une iframe, ou « inline frame » (un « cadre intérieur » en français). L'iframe est une fonction HTML permettant d'appeler dans une page Web une autre page Web. En définissant une largeur et une hauteur de 1x1 pixel, cette page Web est invisible pour l'internaute.

Tout le contenu de la page incluse est chargé, publicités comprises mais encore une fois l'utilisateur ne voit pas les éléments qui se chargent en tâche de fond. Ainsi, un éditeur peu scrupuleux peut berner un adserver en multipliant ses emplacements publicitaires sans submerger son contenu avec des publicités plus ou moins intrusives.

PARTIE 3. VENDRE UN CIBLAGE FICTIF

INTRODUCTION

Le ciblage permet de concentrer ses investissements publicitaires en vue de toucher une cible bien précise.

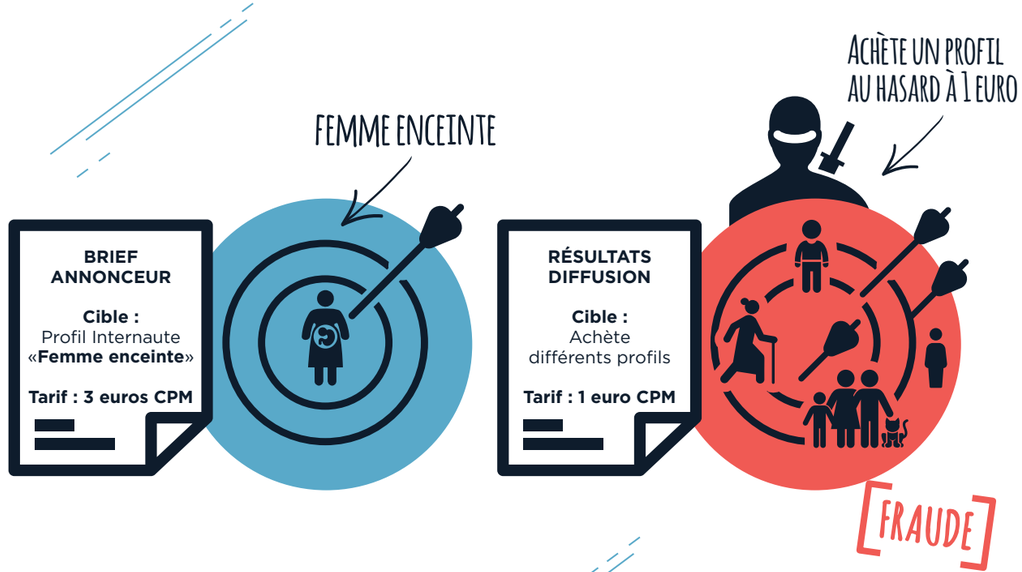
Le ciblage peut être géographique, comportemental, contextuel ou encore sociodémographique.
Il arrive que ces ciblages ne soient pas respectés, volontairement ou non, par les partenaires (agence, régie, trading desk, éditeur, fournisseur de données tierces...). On parle alors d'altération des ciblages.

EN VOICI QUELQUES EXEMPLES

1. LA FRAUDE AU CIBLAGE DE SEGMENTS D'INTERNAUTES

Prenons un exemple : L'annonceur souhaite, pour sa campagne, s'adresser à une audience bien particulière (ex : femmes CSP+ intentionnistes chaussures). Le partenaire lui fait croire qu'il cible des individus en fonction de critères socio-démo et/ou d'intentions. En réalité, la campagne est diffusée sur des sites sans avoir recours à aucun ciblage.
Pour l'annonceur, cela implique une dépense média qui ne correspond pas à son brief initial, ce qui peut jouer sur les performances de sa campagne.

Quelles raisons motivent cette fraude ?
Pour l'acheteur média : il justifie alors un CPM élevé grâce au ciblage de données tierces qualifiées mais ne les utilise pas, achetant donc beaucoup moins cher l'espace publicitaire et augmente donc mécaniquement sa marge. Pour le fournisseur de données : cela lui permet d'augmenter fictivement le prix et le volume de ses segments.



2. LA FRAUDE AU CADRE DE DIFFUSION

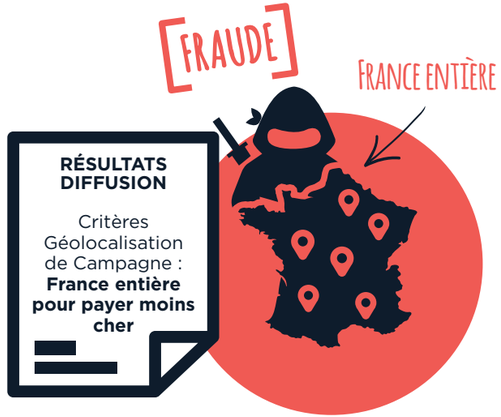
Le partenaire s'engage auprès de l'annonceur à diffuser la campagne sur une liste de sites définie. En réalité, pour diminuer ses coûts d'achat, le partenaire diffuse les bannières sur une liste de sites plus large et/ou différente de la liste prédéfinie. Ceci au risque que les bannières soient visibles sur des sites qui ne sont pas en affinité avec la cible, ou même potentiellement nuisibles à la marque en termes d'image.

> Il faut être en confiance avec son partenaire et lui même doit l'être avec ses partenaires. Ce qui est difficile étant donné le nombre d'intermédiaires. Je ne crois pas au ciblage sur profil (intérêts / Socio) s'appuyant sur des données externes car il faut de la fraîcheur.
> Je regarde l'écart entre nombre de clics et nombre de sessions, le taux de rebond et j'utilise au maximum un pixel d'impression en propre.

Paulo Esteves
Chief digital officier

3. LA FRAUDE À LA GÉOLOCALISATION

Le partenaire s'engage auprès de l'annonceur à diffuser la campagne sur une zone géographique précise (pays, ville, région...). Ce type de ciblage limite généralement la puissance de la diffusion pour le partenaire. Il peut donc arriver que le partenaire diffuse hors de la zone définie pour livrer le volume d'impressions.



4. LE DOMAIN SPOOFING

Le domain spoofing est une fraude à laquelle certains hackers ont recours en programmatique, ceci afin d'usurper le nom de domaine de sites premium. L'agence a le sentiment que ses publicités sont diffusées sur des espaces de qualité alors que dans les faits c'est l'inverse. Les impressions sont générées sur des sites de faible qualité voire même nuisibles à la marque. Le domain spoofing rend les sélections de sites inopérantes, détourne le budget des annonceurs et le revenu des éditeurs usurpés. Le domain spoofing est probablement la fraude la plus insidieuse, la plus lucrative et difficile à détecter.

5. L'USURPATION DU DEVICE

Les émulateurs sont des programmes qui permettent aux développeurs de valider leur travail en émulant différents devices mobiles. Certains fraudeurs utilisent ces émulateurs et changent les en-têtes http de l'hébergement des émulateurs pour se faire passer par n'importe quel autre device et générer de fausses impressions.

6. L'USURPATION DE NOM D'APPLICATION MOBILE

Les noms des applications pouvant changer, il est important de suivre les applications sur lesquelles vous êtes exposés par leur Bundle ID et non par leur nom.

PARTIE 4. VENDRE UN RÉSULTAT FICTIF

INTRODUCTION

Pour mieux valoriser les espaces vendus, le mieux est d'afficher de belles performances dans les outils d'attribution utilisés par les annonceurs.
Et pour être sur de bien performer, le plus simple est de s'assurer que les chiffres affichent la «bonne» vérité.
Le cas ultime est le «vol de conversion» par manipulation de la solution de tracking en place.

Un seul cas présumé a éclaté à ce jour. Il s'agit de l'affaire Steelhouse / Criteo (voir encadré) mais ces pratiques très rares ces dernières années deviennent plus communes et surtout plus sophistiquées. Plus simple, les arnaques au ciblage sont également monnaie courante. Cibler des internautes dont on sait qu'ils achèteront de toute façon est un bon moyen pour un vendeur de valoriser l'espace media qu'il commercialise...
Et pour finir, les vieilles méthodes ont la vie dure. Payer l'internaute pour faire ce qu'attend l'annonceur reste un classique indémodable depuis le début de la publicité online il y a 20 ans.

EN JUIN 2016, CRITEO A PORTÉ PLAINTE CONTRE STEELHOUSE. SI LA PLAINTE EST DÉCRITE COMME PORTANT SUR LA NOTION DE "CLICK FRAUD", IL S'AGIT EN FAIT D'UNE PRÉSOMPTION DE FRAUDE AUX SOLUTIONS D'ATTRIBUTION.

Criteo s'estime floué. En effet, les équipes de Criteo ont le sentiment qu'un grand nombre de ventes attribuées par les annonceurs et leurs systèmes de tracking à Steelhouse le sont à cause d'actions frauduleuses de Steelhouse.

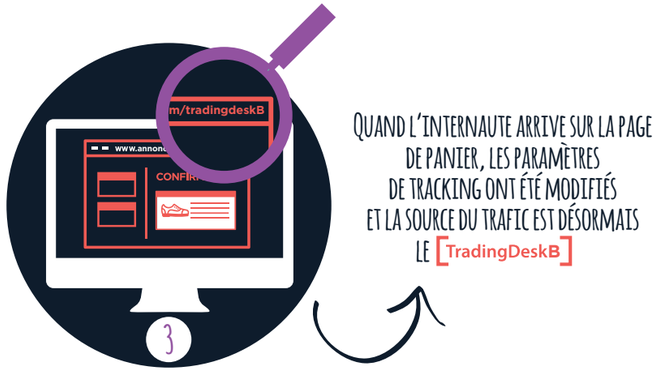
Cette affaire est intéressante car elle est d'un nouveau genre.
Un vendeur de trafic se faisant voler des conversions (qui devraient lui être attribuées) par un autre vendeur de trafic est un cas inédit dans le webmarketing.

Mais les aspects business et légaux ne sont pas les seuls aspects passionnants de ce dossier. En effet, techniquement, plusieurs particularités doivent être notées :
- les risques liés à l'installation de javascript de sociétés tierces dans les pages de l'annonceur. Cela illustre ce qu'il est possible de faire avec un javascript dans une page Web
- la dépendance des annonceurs et de leurs apporteurs de trafic aux solutions d'attribution et donc la tentation pour ces derniers d'essayer de changer les chiffres par tous les moyens
- l'ingéniosité supposée des équipes de Steelhouse qui semblent avoir monté un stratagème optimisé de manière itérative

Steelhouse et Criteo étant arrivés à un accord fin octobre 2016, le grand public n'aura jamais le fin mot de l'histoire, mais la lecture de la documentation juridique écrite par les avocats des 2 sociétés mérite le détour.

1. L'ALTÉRATION DE TRACKING (UTM SOURCE)

L'altération du tracking est une méthode de fraude qui a pour objectif de modifier le résultat d'une campagne pour en améliorer la perception des résultats. Ce type de fraude nécessite de tromper les solutions de tracking pour leur faire attribuer des conversions à une campagne plutôt qu'à une autre.
La méthode la plus connue concerne notamment les solutions d'analytics et d'attribution qui utilisent des paramètres dans les urls. Ceux-ci sont visibles et compréhensibles pour les pirates. C'est le cas des balises utm de Google Analytics, par exemple utm-source et utm-medium. Dans ce cas précis, le pirate va chercher à remplacer le contenu de la variable par le nom de la source de trafic qu'il commercialise. Cela lui permet d'optimiser le nombre de conversions qui sont associées au trafic qu'il génère et ainsi améliorer sensiblement ses chances de continuer à vendre du trafic à l'annonceur concerné, voire lui permettre d'augmenter ses prix.
Techniquement, le pirate exploite un code javascript qu'il a fourni à l'annonceur et que celui-ci a installé dans ses pages. Ce code javascript permet au pirate de changer l'url courante au moment d'un clic de l'utilisateur dans une page de l'annonceur. Le pirate, en changeant l'url courante, modifie le contenu des paramètres indiquant la source de trafic de la visite (par exemple utm-source). Ainsi, pour changer l'url, il peut par exemple utiliser des calques transparents qu'il installe sur les pages du site de l'annonceur grâce à son javascript et sur lesquels l'internaute va cliquer à son insu.
Cette méthode est difficile à détecter côté annonceur. Elle peut être relevée par d'autres fournisseurs de trafic que le pirate car ceux-ci risquent de voir le nombre de ventes qui leur est attribué fluctuer fortement. Le cas le plus connu d'altération de tracking est l'imbroglio judiciaire qui a opposé Criteo à la régie américaine Steelhouse (voir encadré).



2. LES ADD-ONS

Les add-ons sont des logiciels additionnels qui peuvent être ajoutés à un navigateur. Ils peuvent être de types divers : ad blockers, solutions de cashback, outils de download de videos, plug-ins sociaux, outils de débug... Si la plupart de ces add-ons sont utiles et bienveillants, certains ont pour objectif d'altérer la publicité vue par l'utilisateur voire de créer de nouveaux espaces.

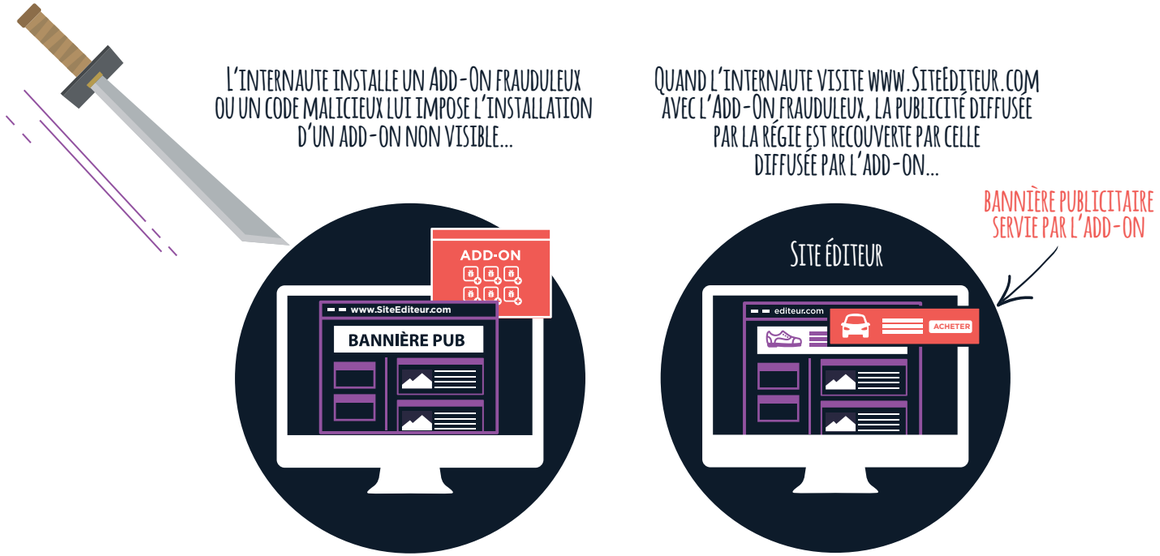
Plus de 130 extensions malveillantes ont été avérées et 4 712 suspectées sur le navigateur Chrome, associées à divers types de fraudes : vol de données (identifiants et mots de passe), redirection vers des publicités frauduleuses ou piratage de comptes sur les réseaux sociaux. L'utilisateur ne peut pas percevoir l'aspect frauduleux de l'extension, qui pour lui est un service qu'on lui propose. Le comportement malveillant de ces add-ons se déclenche uniquement sur certaines pages ciblées au préalable par les concepteurs.

Les extensions de ce type réalisent des appels aux API du navigateur pour avoir accès à diverses autorisations (requête Web, modification de trafic, redirection non désirée, injection de code javascript dans des pages Internet ...). L'utilisateur doit toutefois donner son autorisation à l'extension pour qu'elle puisse bénéficier des données.

Certaines extensions contiennent des balises de localisation leur permettant de communiquer à un serveur à distance tout l'historique et les données de navigation de l'internaute touché. A partir de là, les paramètres d'URL peuvent être modifiés, pour générer par exemple un dépôt de cookie. Les extensions peuvent remplacer des publicités par d'autres ou injecter de la publicité sur des sites qui n'ont pourtant pas d'espaces destinés à cela. Des faux clics ou appels d'affichages peuvent être générés, ainsi que l'installation invisible d'autres malwares.

> La performance est le critère qui permet d'écrémer les fraudeurs. Nous faisons peu de campagnes programmatiques car CPM trop élevé et performance trop faible.

Thomas Hadjadj
Digital Acquisition Marketing Manager
Head of display Europe



3. LE RETARGETING MASQUÉ EN TARGETING

L'annonceur fait appel à un partenaire pour qu'il mette en place une stratégie de targeting (prospection) visant à atteindre une nouvelle audience susceptible d'acheter des produits ou de souscrire des services. Cela implique une exclusion de tous les visiteurs de ces campagnes.

Dans les faits, le partenaire, grâce aux éléments de tracking fournis à l'annonceur pour mesurer les performances, peut identifier, dans certains cas, les visiteurs du site pour les recibler. Le ciblage des internautes (appelé retargeting), permet d'augmenter drastiquement les performances de la campagne en terme de taux de clic et de conversion.

Les raisons incitant le partenaire à avoir recours à cette fraude sont diverses. En cas de compétition avec un autre partenaire, l'objectif serait d'améliorer les performances en vue d'être sélectionné par l'annonceur. Autre raison, diminuer ses coûts d'acquisition peut dans certains cas, lui permettre d'obtenir de nouveaux budgets.

L'impact pour l'annonceur est une mauvaise lecture des performances. En plus de sur-solliciter les visiteurs du site, cette stratégie de prospection ne génère pas de nouveaux visiteurs.

Contrôle avec des outils de tracking : pour détecter du retargeting masqué en targeting, il y a lieu d'étudier le taux de nouveaux visiteurs par le biais d'outils de tracking et le suivre dans le temps.

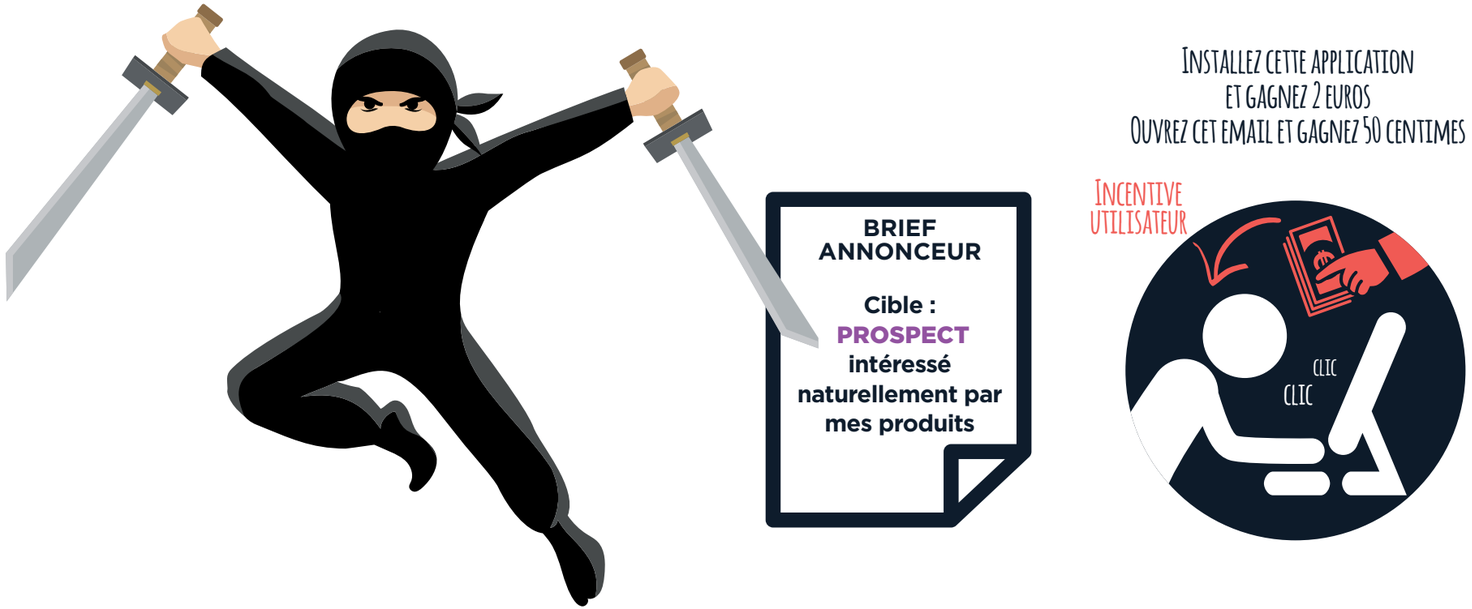
4. LE TRAFIC INCENTIVÉ

C'est peut être la plus vieille fraude de l'Internet publicitaire. Au début des systèmes de liens sponsorisés, des pirates renvendaient déjà du trafic incentivé à Google ou Yahoo ! C'était il y a près de 15 ans et cette fraude continue de perdurer.

Le trafic incentivé peut prendre la forme de pay-to-click (ou crowd sourcing) et d'incentivised ad network. Dans le cas des pay-to-click, les internautes sont rémunérés pour cliquer ou lire des publicités. Quant aux incentivised ad networks, les internautes sont incités à cliquer sur des publicités avec en retour des points de fidélité, des coupons de réduction, des bitcoins.

Le trafic incentivé permet au partenaire d'augmenter les statistiques et d'obtenir des taux de clics ou volume de visites qui en l'apparence semblent être intéressants aux yeux de l'annonceur.

L'annonceur quant à lui n'a pas une bonne lecture des réelles performances de la campagne. Il faut qu'il utilise une solution d'attribution pointue pour détecter les sources de trafic qui ont recours à des fournisseurs de trafic incentivé (voir schéma).



FRAUDE, LE CÔTÉ OBSCUR DU MARKETING DIGITAL

PARTIE 5. LES MAUVAISES PRATIQUES

INTRODUCTION

Dans la diversité des formats publicitaires, il en existe un certain nombre qui s'imposent plus ou moins fortement à l'individu exposé.

Les possibilités d'échapper au message publicitaire sont ainsi réduites. L'individu est insidieusement amené à regarder la publicité, l'humain est ainsi manipulé.

Il y a un écart de maturité important entre les annonceurs, entre ceux qui ne savent pas qu'il faut tracker et ceux qui font la chasse aux robots intelligents. Il faut éviter le plus possible les vices dans les contrats, dans les VU négociés rien ne stipule que ce soit du visiteur humain.

Alexandre Schont
Responsable Business Development

TABMO
CREATIVE MOBILE DSP

1. L'INTERSTITIEL

L'interstitiel est une page publicitaire qui recouvre entièrement l'écran sur mobile. Il s'affiche généralement au moment de l'ouverture d'une application ou en naviguant entre deux pages. Un clic est cependant nécessaire pour le fermer, ce qui peut parfois être difficile à réaliser, au vu de la taille de la croix permettant de fermer le format.

Format très intrusif, la difficulté de le fermer explique ses taux de clics élevés. D'ailleurs, de plus en plus de régies, éditeurs et ad-exchanges refusent la diffusion de ce format.

2. LA VIDÉO NON SKIPPABLE

Le pre-roll non skippable est un message publicitaire vidéo de quelques secondes qui s'affiche avant la visualisation d'une vidéo de contenu. C'est un format qui dure généralement entre 10 et 30 secondes. Format intrusif, la particularité du pre-roll non skippable est qu'il ne peut être passé. L'internaute est contraint de regarder entièrement la publicité, avant que ne s'affiche le contenu recherché. Parfois même, la publicité se met en pause lorsque l'internaute consulte un autre contenu en même temps.

3. L'HABILLAGE ENTIÈREMENT CLIQUABLE

L'habillage est un format publicitaire souvent utilisé à des fins événementielles, qui apparaissait à l'origine uniquement sur la page d'accueil d'un site. Dorénavant, il est utilisé également sur les pages internes d'un site Web. L'absence en général de call to action en haut et sur les deux côtés de la page provoque des clics involontaires de la part de l'internaute. Cela le détourne du contenu de la page qu'il est venu chercher.

4. LE SITE UNDER

Même si cette méthode est de moins en moins utilisée ces dernières années, cela reste une technique de génération de trafic massif.

Le principe est d'ouvrir une page d'un annonceur dans une nouvelle fenêtre du navigateur et sous la fenêtre active. L'internaute ne verra donc cette fenêtre qu'à la fin de sa navigation à la fermeture de son navigateur.

5. LE FOOTER EXPAND

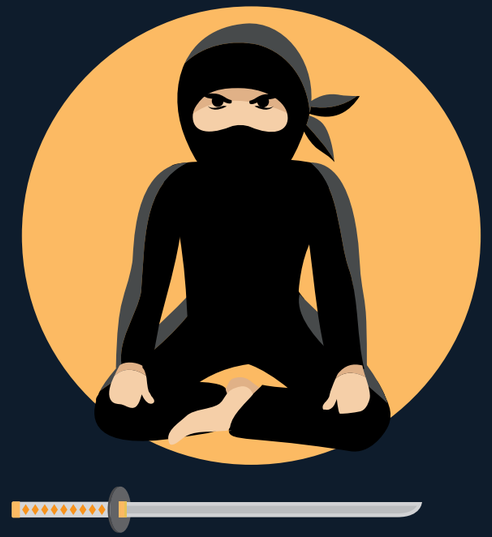
La technologie du footer expand peut déposer un cookie post-clic à l'affichage. Même si ce procédé peut être considéré comme limite, il est principalement le résultat d'un impératif technique. Il convient de passer par une page d'atterrissage dans ce genre de cas pour éviter de se confronter à une certaine confusion dans les reportings.

6. LA NON VISIBILITÉ DES BANNIÈRES

Des emplacements publicitaires peuvent se trouver en dehors de l'écran de l'internaute sans que ceci soit dans un objectif de fraude mais juste dans une logique de monétisation supplémentaire sur des pages qui peuvent être longues.

L'IAB et le MRC ont mis en place une convention marché qui consiste à comptabiliser comme visible une bannière si plus de 50 % de ses pixels sont affichés à l'écran et ceci pendant plus d'une seconde.

PARTIE 6. LES PARADES POUR LUTTER CONTRE LA FRAUDE



PARADES

PARADE MÉTHODOLOGIQUE

Identifier clairement les KPI avant le démarrage de la campagne en fonction de son objectif afin de pouvoir analyser correctement les résultats

- Création de dashboard interne de suivi des résultats
- Utilisation de vos outils analytics pour remplir de dashboard*
- Analyse des résultats en utilisant des KPI adaptés à l'objectif

PROTECTION JURIDIQUE

Prévoir les conditions de prestations dans le contrat afin de pouvoir se retourner contre le prestataire en cas de manquement

- Objectif de la campagne
- Informations présentes dans les reportings
- Utilisation d'outils de contrôle et vérification

PARADE TECHNOLOGIQUE

Utiliser des outils technologiques d'identification de la fraude afin de se prémunir des risques

- Outils de mesure de la visibilité des impressions
- Outils répertoriant des sites blacklistés et des robots
- Outils de Brand Safety

L'IMPORTANCE DE L'ORGANISATION

Prévoir l'organisation interne optimale afin de minimiser les risques : séparer l'opérationnel du contrôle des résultats

- Direction des achats/équipe opérationnelle : responsable de la campagne
- Contrôleur de la campagne : responsable de l'analyse des résultats**
- Prise de décision par le contrôleur de la campagne

* Utiliser des outils Analytics qui montrent la totalité du tunnel de conversion (éviter les outils gratuits qui ne sont pas complets)
** S'assurer que tout le monde parle le même langage, comprend les KPIs de la même manière et comprend les objectifs de la campagne

1. LA PROTECTION JURIDIQUE

Afin de se protéger juridiquement et pouvoir attaquer le prestataire en cas de non-respect des engagements, une attention particulière doit être accordée au contrat pour y retrouver ces engagements.
Par exemple, les objectifs et les livrables attendus doivent être clairement définis et précisés dans le contrat avec le prestataire (agence, régie ou autre).
Si l'annonceur souhaite imposer l'usage d'outils de contrôle et vérification (contrôle d'espaces et de visibilité), cela doit également être précisé dans le contrat.
Nous pourrons donc trouver des contraintes dans le contrat comme pouvoir accéder aux sources d'inventaires et à la qualité de leur audience, préciser si l'extension d'audiences est autorisée, pouvoir connaître les dépenses réelles précises sur chacune des sources ou devoir respecter un taux de nouveaux internautes ou nouveaux clients dans le cas où le retargeting n'est pas ouvert.

LOI SAPIN : PUBLICITÉ PROGRAMMATIQUE

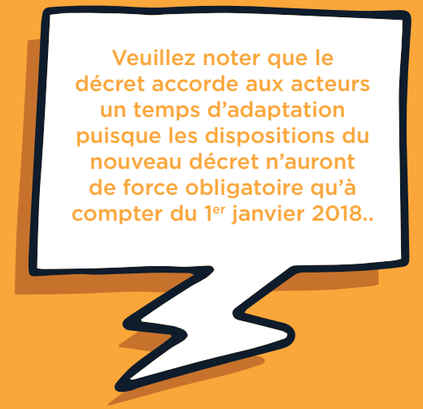
Le décret d'application n°2017-159 du 9 février 2017 est récemment venu préciser la loi relative à la prévention de la corruption et à la transparence de la vie économique et des procédures publiques dite « Loi Sapin » (Loi n°93-122 du 29 janvier 1993) afin notamment de tenir compte des nouvelles pratiques d'intermédiation en matière de publicité programmatique.

EN RÉSUMÉ, LES 3 POINTS ÉVOQUÉS :

I - L'inclusion de la publicité digitale et des pratiques d'achats programmatiques dans le champ d'application de la Loi Sapin
La loi s'applique désormais formellement aux activités d'optimisation du ciblage publicitaire en ligne.
Le média digital comme support publicitaire et les pratiques d'intermédiation par le biais de systèmes automatisés relèvent donc désormais expressément de la Loi Sapin.

II - La transparence dans la publicité digitale : les obligations de compte rendu.
Le décret impose des obligations spécifiques de compte rendu en matière de publicité digitale.

III- Les dérogations au champ d'application territorial
Le décret n'est pas applicable aux Supports (et leurs régies) établis dans un autre Etat membre de l'Union européenne ou partie à l'Espace économique européen dès lors qu'ils sont assujettis à des « obligations équivalentes » de compte rendu, en vertu de dispositions nationales.



2. LA PARADE MÉTHODOLOGIQUE

Avant de lancer une campagne digitale avec un partenaire, il est important de respecter plusieurs étapes afin de pouvoir bien suivre les résultats et de bien veiller au respect des attendus.
La 1ere étape consiste à créer des dashboards qui vous permettront de suivre et surveiller.
Ces dashboards vont permettre de retrouver des indicateurs comme :

- Taux de clic
- Taux de rebond
- Nombre de pages vues
- Temps passé sur le site
- Taux de nouvelles sessions
- Taux de transformation
- Taux de nouveaux clients
- Répartition de l'origine du trafic

La 2ème étape consiste à imposer l'utilisation de votre outil Analytics pour vous permettre d'alimenter ce dashboard avec le niveau de granularité le plus fin :

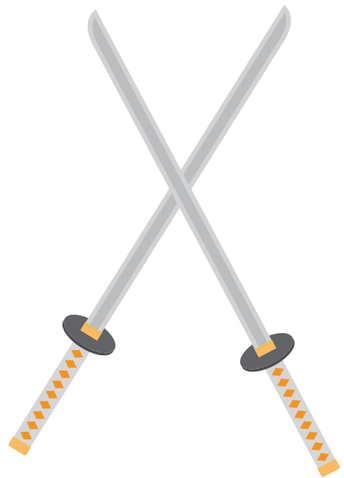
- Par campagne
- Par source d'inventaire
- Par support

Ensuite, vous allez pouvoir analyser les résultats sur ce dashboard avec un principe permanent de comparaison des résultats des différentes campagnes pour pouvoir mettre en évidence des résultats anormaux.

3. L'IMPORTANCE DE L'ORGANISATION

L'organisation des équipes chez l'annonceur est un point déterminant dans la lutte contre la fraude.
Comme dans les fonctions de contrôle des risques de marché dans les banques, il faut séparer la personne qui est responsable de la campagne (donneur d'ordre des achats médias) de la personne qui contrôle les résultats (conserver le côté garde-fou).

Même si les niveaux peuvent être variables, il faut internaliser au maximum les expertises pour permettre de parler le même langage que les partenaires et pouvoir suivre leurs actions.
Cette expertise doit avoir un pouvoir de décision plus important que la direction des achats dans l'allocation des budgets de façon à ne pas laisser le coût comme seul élément d'arbitrage.



4. LA PARADE TECHNOLOGIQUE

La dernière catégorie des parades concerne les technologies de contrôle de la fraude.
Certaines technologies vont vous permettre de surveiller la visibilité des impressions de votre campagne.
Que ce soit sur les ordinateurs ou sur le mobile, ceci permettra de couvrir différents cas de fraudes.

D'autres technologies vont vous permettre de bénéficier de la mutualisation des surveillances anti-fraude.
Ces partenaires technologiques maintiennent des listes d'adresses IP ou de sites blacklistés (un peu comme un antivirus maintient et enrichit en permanence une liste de virus).

La détection s'appuie sur des algorithmes ou des études humaines :

- Détection d'anomalies pour repérer des comportements anormaux caractéristiques des bots (vitesse de navigation anormale, schémas de navigation récurrents ...)
- Analyse des navigateurs : les robots utilisent de faux navigateurs. Grâce à un script implémenté dans l'adserver, la solution analyse en temps réel les caractéristiques du navigateur utilisé pour les relier à des caractéristiques connues. Les paramètres différents ou manquants permettent ainsi de dégager des comportements frauduleux.
- Etude préalable par des ingénieurs puis détection des 'signatures' de malwares ou bots
- Observation proactive des forums et communautés de fraudeurs

Dans le cas de campagnes pour votre application mobile, des technologies vont permettre d'identifier le faux trafic en analysant :

- Les adresses IP : si la même adresse IP revient trop fréquemment dans les téléchargements
- Les ID des devices : si le même device ID est à l'origine de plusieurs téléchargements
- Les noms des mobiles (« iPhone de Victor », etc.) : si le même nom revient plusieurs fois
- Les types/marques de mobile : si un gros volume de téléchargements est généré sur un seul type de téléphone
- Le délai entre le clic et l'installation : s'il est trop court

On identifie du trafic détourné, c'est-à-dire de qualité non désirée en regardant :

- L'horaire moyen de l'action ou l'utilisation de VPN : pour vérifier le fuseau horaire
- Les mobiles jailbreakés : pour identifier du trafic non comptabilisé par les Appstores
- Les taux de conversion suite à l'installation au sein de votre application : pour identifier du trafic incentivé

Les acteurs principaux dans ce domaine sont :

Nous vous conseillons de consulter le panorama des outils techniques contre la fraude :
http://www.journaldunet.com/ebusiness/publicite/1185990-fraude-publicitaire-les-techniques-et-les-acteurs-pour-y-remedier/
Pour garantir leur fiabilité, l'unique critère existant à ce jour est l'accréditation accordée par le Media Rating Council (MRC), association américaine indépendante dont la mission est d'assurer la validité et l'efficacité des outils de mesure d'audience.

Dans le cas de budget au CPM, nous imposons à nos partenaires Display d'utiliser une solution comme IAS ou Adloox.
Pour contrôler les ciblages et éviter l'AdStacking, nous nous appuyons sur l'Analytics pour vérifier : le taux de rebond, le temps passé sur le site, le nombre de pages vues, l'origine des IP, les profils des internautes.
Pour limiter la fraude, nous utilisons des Deals garantis (programmatique garanti).

Grace Paynot
Responsable Marketing Digital,
CRM et Communication

PSA BANQUE

ADS.TXT

«En 2017, l'IAB (Internet Advertising Bureau) a lancé, via l'IAB Tech Lab, l'initiative ADS.TXT (ADS pour Authorized Digital Sellers), qui se matérialise sous la forme d'un fichier texte placé à la racine d'un domaine où se trouvent des emplacements publicitaires et qui précise ses identifiants de vendeur sur les différentes places de marché ainsi que différentes informations permettant aux acheteurs de s'assurer qu'ils achètent bien sur le domaine qu'ils comptent cibler et non pas sur un emplacement utilisant le «domain spoofing»

Cette initiative va dans le bon sens et contribuera certainement à rendre l'écosystème plus transparent. Pour en savoir plus :
https://iabtechlab.com/ads-txt-about/

Ad-Exchange* :

L'Ad-exchange est une plateforme automatisée de vente et d'achat d'espaces publicitaires sur Internet. Elle permet de mettre en relation des acheteurs (DSP, agences de publicité, agences médias ou annonceurs directement) et vendeurs (SSP, sites supports éditeurs, réseaux ou régies publicitaires).

Les Ad-exchanges sont une des composantes techniques fondamentales du Marketing programmatique. (source wikipedia)

Un ad-exchange est une plateforme automatisée de vente et d'achat d'espaces publicitaires Internet sur laquelle se rencontrent les demandeurs d'espaces (annonceurs, agences média et réseaux de reciblage) et les offreurs (sites supports éditeurs, réseaux, régies). Sur un ad-exchange, l'activité de vente / achat des espaces publicitaires se fait généralement en RTB.

Un ad-exchange permet d'automatiser quasiment totalement les phases de négociations / achats et celles d'implémentation des campagnes. Sur un ad-exchange une campagne peut être mise en place sans qu'à aucun moment il n'y ait un contact direct entre le vendeur et l'acheteur d'espaces publicitaires. La vocation d'un ad exchange est donc de réduire les coûts de fonctionnement du marché.

Un ad-exchange se finance par une commission sur les échanges très inférieure à celle prélevée habituellement par une régie et éventuellement par des droits d'inscription des utilisateurs.

Dans le cadre d'une plateforme automatisée, les éditeurs fixent un prix minimum pour leurs différents emplacements publicitaires disponibles et éventuellement un filtre sur les annonceurs acceptés. Les annonceurs ou agences créent leurs campagnes en choisissant leurs formats, leurs critères de ciblage et un prix d'enchère au CPM ou plus rarement au CPC.

L'ad-exchange compare en temps réel l'offre et la demande et peut diffuser, selon les cas, les campagnes en temps réel impression par impression ou par blocs d'impressions.

SSP* :

SSP est l'acronyme pour Sell Side Platform ou Supply Side Platform. Une SSP est une plateforme permettant aux éditeurs d'automatiser et d'optimiser la vente de leurs espaces publicitaires.

Ces plateformes sont utilisées par les grands éditeurs pour commercialiser les espaces n'ayant pu être commercialisés de manière traditionnelle par leur régie interne ou externe et éventuellement par des éditeurs plus modestes pour commercialiser l'intégralité de leur inventaire publicitaire.

Les SSP diffusent l'inventaire disponible de leurs éditeurs auprès des différents ad-exchanges du marché et éventuellement auprès d'ad-networks et autres DSP.

Les SSP les plus avancées opèrent en temps réel. Lorsqu'un emplacement publicitaire est appelé lors de la consultation d'une page sur un site éditeur, la plateforme recherche la meilleure offre faite sur ce type d'emplacement et pour le profil de visiteur détecté et diffuse automatiquement la publicité correspondante.

Les SSP ont normalement pour vocation de diminuer la part des invendus et de favoriser l'augmentation du CPM des éditeurs utilisateurs.

DSP* :

DSP est l'acronyme pour Demand Side Platform. Une plateforme DSP est un service permettant aux annonceurs, trading desks et agences d'optimiser leurs achats d'espaces publicitaires display.
L'achat par une plateforme d'optimisation se fait essentiellement sur les différents ad-exchanges du marché.
Les plateformes DSP fonctionnent généralement en temps réel dans une logique RTB. Lorsqu'une campagne est programmée et définie à travers ses critères de ciblage par un acheteur, la plateforme d'optimisation recherche les impressions disponibles au meilleur coût.
Une plateforme DSP peut également réaliser en cours de campagne des adaptations pour sélectionner les créations, supports et critères de ciblage assurant les meilleurs retours sur investissement en fonction des objectifs de campagnes (clics, conversions, etc..). Certaines solutions vont jusqu'à analyser les contenus et montants des ventes générées dans leur processus d'optimisation.
Les DSP sont le pendant coté acheteurs des SSP coté sites éditeurs supports.

Extension d'audience* :

L'extension d'audience est la pratique par laquelle un site Internet dont l'audience est particulièrement recherchée par les annonceurs et qui vend généralement tous ses espaces publicitaires peut proposer à un annonceur d'aller toucher son audience habituelle sur d'autres sites à travers un réseau spécialisé.
L'extension d'audience repose sur le même principe que les techniques de reciblage.

Trading Desk* :

Un trading desk est, dans le domaine de la publicité Internet, une structure qui prend en charge l'achat de l'espace publicitaire Internet sur les ad-exchanges pour le compte des annonceurs. Les services d'un trading desk sont délivrés à partir d'une plateforme technique (DSP et développements spécifiques) et d'une équipe technique et marketing spécialisée dans l'achat d'espaces RTB.
En général, le trading desk réalise l'achat directement sur les sites éditeurs ou ad-exchanges (marketplaces publicitaires) en ayant le plus souvent recours au RTB. Le trading desk optimise l'achat publicitaire en intégrant l'analyse des performances et l'utilisation éventuelle des différentes données (first party data, données éditeur, 3rd data). Il ne recherche donc pas forcément le CPM le plus bas.
L'individu en charge de la planification et de l'optimisation des campagnes au sein d'un trading desk est un trader media.
Les trading desks peuvent être intégrés dans une agence média, être totalement indépendants et avoir été créés ex-nihilo ou même être montés en interne par de gros annonceurs.

RTB* :

RTB est le sigle couramment utilisé dans le domaine de la publicité Internet et probablement de plus en plus dans le domaine des médias « traditionnels » pour désigner le principe des enchères en temps réel ou « real time bidding ».
Dans le cadre du RTB display une impression publicitaire est mise aux enchères en temps réel sur une place de marché (ad-exchange, plateforme programmatique, etc.) lorsqu'un internaute ou mobinaute consulte une page Web ou une application mobile. Sauf exceptions et accords particuliers, c'est alors l'annonceur produisant l'enchère la plus haute qui voit sa création diffusée. Selon les cas l'enchère peut avoir été pré-établie ou être déterminée en un dixième de seconde par un algorithme pre-bid.
Le RTB est initialement associé aux achats programmatiques Internet, mais tous les achats programmatiques ne sont pas faits en RTB. L'usage du RTB dans les processus d'achat d'espace publicitaire digital est en hausse constante et n'est plus comme à l'origine réservé aux espaces de qualité secondaire.

Programmatique garanti :

Le programmatique garanti est un mode d'achat d'espace publicitaire automatisé (programmatique) par lequel l'espace publicitaire vendu n'est pas mis aux enchères en RTB, mais vendu au préalable à un annonceur par le biais d'un « private deal ». On parle également de programmatique direct.
Le terme de programmatique direct est essentiellement utilisé dans le contexte de la vente d'espaces digitaux dont une bonne part se fait désormais en mode programmatique. L'usage du terme peut cependant aussi s'appliquer aux médias traditionnels qui sont également gagnés par les modes de gestion programmatiques.

Yield Management :

Dans le domaine de la monétisation publicitaire, le yield management est la pratique qui consiste à optimiser les revenus publicitaires par l'adoption d'un mode de tarification plus ou moins dynamique qui s'adapte à la demande des agences et annonceurs.
Le yield management pratiqué par une régie publicitaire peut concerner la plupart des médias publicitaires.
C'est dans le domaine de la publicité digitale que le processus peut être le plus abouti puisque sur les plateformes programmatiques l'adaptation du tarif peut se faire en temps réel et impression par impression en fonction des enchères des annonceurs (RTB). Lorsque cette optimisation des revenus se fait en englobant à la fois les modes de commercialisation directs avec des espaces vendus en garanti et la vente en RTB, on parle alors de processus de yield holistique.
Sur les médias publicitaires traditionnels, la notion de yield management s'en tient souvent à la création de tarifs spécifiques pour des réservations de dernière minute ou pour les périodes creuses. Cependant, la digitalisation des médias traditionnels (TV programmatique, DOOH programmatique, etc) devrait progressivement développer l'usage d'un yield management plus dynamique et plus automatisé et la notion de yield management holistique pourrait également concerner ces médias.

AdServer full-stack :

Un adserver full-stack est un terme parfois utilisé pour désigner une plateforme gérant à la fois des fonctions de commercialisation en RTB et des fonctions classiques d'ad trafficking d'un ad server.
L'adserver full-stack va donc bien au delà d'un « simple » adserver.
C'est une solution technique de gestion et monétisation des espaces publicitaires qui combine la gestion du trafic management, les procédures de commercialisation en RTB et les modes classiques ou historiques de commercialisation (vente directe, opérations spéciales, etc.).
Une plateforme full-stack doit théoriquement permettre de supprimer la superposition de différentes solutions techniques (adserver + SSP + Adexchange) et d'optimiser la monétisation à travers un processus appelé yield holistique.

Blind Network :

Un blind network est un réseau publicitaire Internet ou mobile sur lequel les annonceurs achètent de l'espace publicitaire sans savoir sur quels sites seront diffusées leurs annonces.
L'achat se fait à l'aveugle car le réseau est composé soit d'un grand nombre de sites à faibles inventaires, soit de sites importants qui ne souhaitent pas que les annonceurs sachent qu'ils « bradent » leurs invendus publicitaires habituellement vendus à des CPM « supérieurs ».
Même si les sites supports utilisés ne sont pas communiqués aux annonceurs, les blind networks peuvent cependant proposer des options de ciblage thématique.
Les blind networks commercialisent généralement les espaces auprès des annonceurs à la performance ou à des CPM très bas.

Header Bidding :

Le header bidding est un processus interne de gestion publicitaire qui permet aux éditeurs d'offrir aux enchères des impressions publicitaires digitales à un plus grand nombre d'ad-exchanges, SSP ou trading desks et de mettre ces acheteurs potentiels en concurrence avec la voie habituelle / interne de commercialisation.
On utilise le terme d'header bidding car le procédé se fait par une insertion d'un ou plusieurs codes spécifiques (tags) dans le header de la page Web hébergeant la création publicitaire.

DMP :

DMP est l'acronyme pour Data Management Platform ou plateforme de gestion des données. Il s'agit d'une plateforme proposée généralement en mode SaaS et permettant de récupérer, centraliser, gérer et utiliser les données relatives aux prospects et clients.
Les premières DMP étaient centrées sur les données de navigation Internet et utilisées à des fins de publicité comportementale. Désormais, les DMP les plus évoluées intègrent les différents points de contact pour la collecte de données et le ciblage marketing et réunissent le offline et le online en utilisant notamment des procédures de CRM onboarding.
Les données gérées par une DMP peuvent également être enrichies par des données en provenance de tiers « spécialistes de la data ».
Les données gérées par une DMP sont utilisées pour optimiser le ciblage et l'efficacité des campagnes marketing et publicitaires et à des fins éventuelles de personnalisation sur les sites Web et applications mobiles.
La DMP peut être vue comme l'héritière de la « traditionnelle » base de données clients et devient un pilier du CRM à travers notamment la mise en place d'un référentiel client unique.
Les DMP proposent de nombreux types de services ou fonctionnalités aux entreprises utilisatrices dont certaines s'étendent à la gestion des prospects et audiences publicitaires dans une logique de PRM (Prospect Relationship Management). Une partie du ROI liée à la mise en place d'une DMP peut potentiellement être réalisée par le biais de l'activation des données.
Quelques exemples de fonctions d'une DMP :
- Analyse et qualification d'audience
- Services de data exchange
- Ventes de données à des sites ou réseaux tiers
- Utilisation des données pour le ciblage multicanal
- Services d'extension d'audience
- Outils de protection des données
- Mesure du ROPO (Research Online Purchase Offline)
- Mesure du ROI offline des investissement digitaux

First Party Data :

Les first party data désignent, dans le domaine de la publicité Internet, les données potentielles de ciblage qui sont collectées directement par le site éditeur support publicitaire. Les first party data sont généralement des données comportementales ou déclaratives enregistrées sur le site support lors de visites précédentes et qui sont associées aux visiteurs à l'aide d'un cookie.
Le terme de first party data s'est ensuite élargi à l'ensemble des acteurs Internet et désigne donc l'ensemble des données « propriétaires » dont dispose une entreprise ou un annonceur. La notion de first party data désignait à l'origine essentiellement les données collectées online, mais elle englobe aussi désormais les données CRM / offline, notamment quand celles-ci sont réconciliées avec les données Internet au sein d'une DMP par

une procédure de CRM onboarding.

Third Party Data :

Les third party data sont généralement des données de ciblage publicitaire ou marketing Internet qui sont fournies à l'annonceur par une société tierce autre que l'éditeur utilisé comme site support pour une campagne.
Les third party data sont essentiellement fournies par des régies publicitaires, des spécialistes de la donnée ou par le biais de procédures de data exchange sur des data marketplace. Ces données comportementales ou déclaratives sont collectées et associées aux visiteurs à l'aide de cookies.
Sur un site e-commerce, les third party data peuvent par exemple être utilisées pour personnaliser l'offre alors que c'est la première fois que l'internaute visite le site.
La notion de third party data a été popularisée par les usages du marketing digital, mais les données externes peuvent également avoir une provenance offline (données sorties de caisses de partenaire, données d'enrichissement B2B, etc).

CRM onboarding :

Le CRM onboarding est la pratique par laquelle on utilise les données offline d'un CRM pour être capable de retrouver et toucher une partie de ses clients dans l'environnement Internet / digital.
Dans le cadre d'un processus de CRM onboarding, la base clients / CRM d'une entreprise est uploadée sur une plateforme d'onboarding et les enregistrements sont comparés (matching) à des bases d'individus identifiés par un cookie ou un identifiant mobile. Les individus en commun entre la base CRM de l'entreprise et ceux des bases utilisées par la plateforme d'onboarding pourront désormais être ciblés par l'entreprise dans l'environnement Internet grâce à un cookie ou un autre type d'identifiant numérique. Il s'agit en quelques sortes de « digitaliser » les données purement offline du CRM.
Le CRM onboarding permet aux entreprises de retrouver, reconnaître et cibler leurs clients sur Internet sans qu'ils aient forcément déjà utilisé ou visité un site de cette entreprise ou lorsque le cookie n'est plus opérant.
La pratique permet également de reconnaître sur le site de l'annonceur des individus clients ne s'étant jamais identifiés ou loggués.
Dans le cadre d'un processus de CRM onboarding, tous les clients ou prospects présents en base ne peuvent être retrouvés et se voir affecté un identifiant numérique. On considère généralement que le taux de matching est le plus souvent compris entre 30 et 50 %.

DCO :

DCO est l'acronyme anglais pour « dynamic creative optimization ». La DCO est donc la pratique par laquelle des créations publicitaires digitales (bannières, publicités Facebook, vidéos, etc.) sont en temps réel automatiquement optimisées au fur et à mesure de leur diffusion. La DCO vise à maximiser le taux de clics et / ou le taux de conversion sur le site de l'annonceur.

Le premier niveau de DCO qu'on appellera ici « DCO simple » consiste « simplement » à adapter en temps réel la création publicitaire en fonction des éléments de contexte relatif à l'individu ciblé (données individuelles, localisation, etc.) ou au contexte d'environnement (heure, météo, etc.). De très nombreuses créations peuvent alors être produites et elles peuvent même être uniques dans le cas par exemple d'une distance point de vente s'affichant dans le message.

*source : www.definitions-marketing.com

En résumé, pour détecter l'ampleur de la fraude dont l'annonceur est potentiellement victime, ce dernier dispose de deux approches couplées qui permettent d'évaluer la qualité de ses investissements digitaux :

Une approche purement quantitative d'analyse et de croisement des données disponibles dans les outils d'analytique et d'attribution, les serveurs de publicité (Adserver), les plateformes de ventes aux enchères de publicité ainsi que les outils de gestion d'achat programmatique (DSP) afin de détecter des métriques ne correspondant pas aux valeurs attendues ou des variations incohérentes. Une approche plus qualitative d'analyse des processus de mise en place des campagnes par l'annonceur et ses agences (briefing, reporting, choix des KPI [indicateurs clés de performance], objectifs, cibles, etc.) afin de contextualiser et comprendre les données analysées.

En termes de recommandations à mettre en œuvre, les principales actions sont :

1) Internaliser l'accès et le stockage des données pour les conserver et les analyser.

2) Définir des processus de pilotage de la fraude au sein de l'annonceur (équipe dirigeante, marketing, digital…) et de l'agence (reporting, choix des éditeurs, blacklisting de sites,…).

3) Disposer d'experts internes capables de vérifier la cohérence des performances et de les analyser dans le détail.

4) Intégrer des outils technologiques d'analyse du mix media et du trafic, tout en étant vigilant sur le rapport entre performance et coût.

Pour chaque recommandation proposée, il importe d'évaluer les moyens et ressources (internes ou externes, outils, processus…) à mobiliser grâce à une analyse sur le rapport entre coûts complets et impacts afin de hiérarchiser les actions à mener. Il est important de souligner que ces actions ne permettront pas de réduire à néant la fraude, ce qui est un objectif inatteignable, mais plutôt de circonscrire la fraude et d'en limiter le volume.

Il est paradoxal de penser que la part de fraude est plus importante dans la publicité digitale que dans la publicité traditionnelle, alors même que la promesse de la publicité digitale est la totale transparence des investissements médias : identification de la publicité utilisée, du site de diffusion, de l'internaute ciblé (par le biais des cookies), de sa visibilité et de la mesure de la conversion pour chaque publicité achetée.

Dans les faits, c'est l'infinie granularité et la complexité afférente de l'achat d'espaces sur Internet qui ouvre un espace de possibilités à ceux qui voudraient frauder en matière de publicités sur le Net. Cette granularité fait la force de la publicité sur Internet qui rend difficile de contrôler l'ensemble des publicités achetées et leur conformité aux commandes de l'annonceur. Les outils de contrôle et de mesure pour limiter la fraude en matière de publicité digitale existent, mais seuls, ne suffiront pas. Le succès dépend de la coopération de l'ensemble des acteurs de la filière: annonceurs, agences, vendeurs d'espaces et fournisseurs de solutions technologiques. Il importe de prendre le sujet de la fraude à bras-le-corps pour l'avenir de l'écosystème Internet et pour préserver la confiance des acteurs.

Livre Blanc - Fraude, le côté obscur du Marketing Digital
Date de parution : Septembre 2017

Contacts :
Collectif de la Performance & de l'Acquisition
8 rue Saint Fiacre
75002 Paris - France

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

Noella Boullay : Déléguée Générale - nboullay@cpa-france.org
Joy Grand : Chargée de Communication - jgrand@cpa-france.org

Un remerciement
tout particulier à Joy Grand

Conception graphique :
Flavie Ferrari
www.flavieferrari.com
06 51 02 70 70

Un merci tout particulier
pour la relecture à :

Gregory Bocquenet
Chief Sale Officer
CibleClic SAS

Julien Dugaret
CEO
Beyable

Rahim Daouadji
Business Developer
Chameleon Ad

Timothée Le Roy
Responsable Marketing
et Communication – Matlo

Oualid Barbouchi
CEO and Co-founder
PRM Factory

Aux membres du Conseil d'Administration du CPA :

À PROPOS DU CPA :

Créé en 2008, le CPA (Collectif de la Performance et de l'Acquisition) est le syndicat professionnel des acteurs du marketing digital à la performance, secteur d'activité constituant le socle de toute stratégie d'acquisition digitale.

Le CPA représente des Editeurs et Prestataires experts, offrant des solutions indépendantes et sur mesure aux décideurs du marketing digital (annonceurs et e-marchands) afin de soutenir leur développement.
Par son action (Livres blancs, Chartes de qualité, Recommandations, Evènements & Networking), le CPA répond à quatre objectifs principaux :

- Réguler un marché foisonnant et en mutation permanente,
- Informer sur les meilleures pratiques de l'acquisition digitale,
- Assurer leur mise en oeuvre dans l'application du cadre légal,
- Représenter les droits et intérêts de ses membres.

Face à la multiplication des modèles d'acquisition et aux parcours utilisateurs toujours plus complexes, les membres du CPA s'engagent à mettre leur expertise, leur compréhension du secteur et leur esprit d'innovation au service de leurs clients.
Le CPA fédère les principaux acteurs du marché du marketing digital à la performance qui représente 10 000 emplois et un chiffre d'affaires de 2,3 milliards d'euros.