Comment se prémunir de la fraude publicitaire sur mobile ?

Les applications mobiles séduisent toujours plus d'utilisatrices et d'utilisateurs. Ce que les annonceurs ont bien compris puisqu'ils y multiplient les campagnes de publicité. Mais la croissance du secteur est menacée par la fraude, laquelle prend chaque année plus d'ampleur, alors même que de bonnes pratiques permettent de lutter efficacement contre le phénomène.

Temps de lecture : minute

---

19 mars 2019

La fraude publicitaire, ce fléau des temps modernes. Avec le développement du numérique, aussi bien du côté des médias en ligne que des startups qui proposent des applications, l'affichage publicitaire a radicalement changé. En 2017, près de 200 milliards de dollars ont été dépensés dans la publicité numérique, dont quatre milliards uniquement en France. De telles sommes attisent forcément les convoitises, et pas toujours les meilleures intentions. La fraude publicitaire n'a ainsi cessé de croître ces dernières années, jusqu'à devenir la némésis absolue des annonceurs, qui ont perdu à cause d'elle près de 7,2 milliards d'euros en 2016, selon les chiffres de la Fédération mondiale des annonceurs (FMA), et qui pourraient représenter, au bas mot, près de 50 milliards de dollars d'ici 2025.

Les applications, qui drainent une part non négligeable de la publicité numérique et bénéficient d'une certaine viralité, cristallisent l'attrait des fraudeurs, au grand dam des entrepreneures et entrepreneurs parfois bien démunis face au phénomène. Comment faire pour se prémunir de la fraude et que faire lorsque l'on en est victime ? Petite série de conseils,

extraits du Guide d’experts de la fraude publicitaire mobile rédigé par Adjust, spécialiste du sujet.

Faire preuve de vigilance et de réactivité

Pour pouvoir identifier le remède adéquat, encore faut-il savoir poser un diagnostic pertinent. D’autant que les fraudeurs usent de diverses techniques pour parvenir à leurs fins. On peut regrouper la majeure partie des types de fraudes en deux catégories. La première catégorie concerne la fraude liée à la falsification de l’ensemble du parcours utilisateur, en essayant de manipuler l’intégralité des points de données, du visionnage d’une publicité à l’installation de l’application, mais également à l’activité de l’utilisateur post-installation. Dans cette catégorie figure notamment l’usurpation de SDK (Software Development Kit, ndlr), les fermes de clics, l’usage de bots, etc. La seconde catégorie relève de la fraude liée uniquement à l’interaction entre l’utilisateur et la ou les publicités. Dans cette catégorie, on retrouve des concepts comme le click spamming ou l’injection de clics.

Pour pouvoir agir rapidement, il est nécessaire d’inspecter régulièrement l’activité des utilisateurs au sein de l’application, afin de vérifier si elle correspond à l’activité d’utilisateurs réels, ou bien s’il s’agit en réalité de faux utilisateurs, des bots par exemple. Un taux de clic anormalement élevé ou concentré sur une période très courte doit vous alerter. Car c’est bien là le problème des pirates, qui recourent à des robots pour faire le sale boulot : difficile, voire impossible pour ces bots d’imiter les interactions humaines et donc de les répartir temporellement de sorte qu’elles soient plausibles… Une fois l’erreur repérée, libre aux éditeurs de ne pas attribuer le trafic généré aux sources qui s’en prévalent pour éviter de nourrir la bête.

Un autre moyen de déceler une anomalie potentielle consiste à surveiller les adresses IP de la source de téléchargement. En effet, les adresses

utilisant un VPN ou le réseau de connexions anonymes Tor, mais aussi celles provenant d'un data center sont l'apanage des fraudeurs, alors que les véritables clients présentent des adresses liées à un opérateur mobile ou à un réseau wifi. Une fois les adresses frauduleuses identifiées et listées, il faut ensuite les blacklister pour éviter les abus.

Collaborer avec les autres acteurs du secteur

Ce travail de recensement des sources malveillantes, de nombreuses entreprises le réalisent de manière plus ou moins structurée. N'hésitez pas à vous rapprocher d'autres acteurs de la publicité pour partager ce qui constitue une base de données des fraudeurs. Cela vous permettra de mieux les repérer et de pouvoir réagir plus rapidement… voire de manière automatique si vos outils le permettent.

Une nécessaire collaboration que ne manque pas d'appuyer la Fédération mondiale des annonceurs, qui recommande par exemple de privilégier ou tout du moins de s'inspirer des outils open source. La structure cite en exemple le domaine du spam email, qui a longtemps constitué une porte d'entrée privilégiée par les fraudeurs. " *Même les éditeurs de logiciels les plus importants et respectés aujourd'hui utilisent les mêmes solutions ouvertes comme bases des logiciels propriétaires qu'ils vendent* ", souligne la fédération pour promouvoir le recours à des solutions communes.

Attention aussi si vous travaillez avec une myriade de fournisseurs ou de sous-traitants : exigez d'eux le même niveau de sécurité que celui que vous adoptez en interne. À quoi servirait de mettre en place des standards internes très contraignants si vos partenaires ne sont pas soumis aux mêmes obligations ? Ne mettez pas en péril votre démarche en étant peu regardant sur les entreprises avec lesquelles vous travaillez !

Faire appel à des experts

Une bonne connaissance de la fraude en interne permet de prendre des décisions plus éclairées quant aux bonnes pratiques à mettre en place et à la réaction à adopter en cas d'attaque. Cela passe notamment par le recrutement d'un ou plusieurs experts de la question, capables de cerner au mieux les enjeux de la lutte contre la fraude. Une précaution doublement nécessaire : cette personne ou cette équipe doit être chargée de centraliser les informations sur le sujet, mais aussi d'harmoniser les pratiques internes pour réduire les risques.

La cybersécurité reste cependant une expertise pointue et il peut être recommandé de recourir aux services d'une société spécialisée pour vous guider dans vos démarches. La suite de prévention de la fraude éditée par Adjust permet ainsi de traiter les données d'attribution des applications pour anticiper la fraude et préserver les budgets publicitaires. La tâche peut en effet se révéler ardue à industrialiser.

Mais la meilleure façon de lutter contre la fraude ne serait-elle pas de rendre l'objet du délit moins attractif pour les fraudeurs ? En revoyant certains objectifs d'investissement ou de diffusion à la baisse ou en favorisant des campagnes plus réduites, les annonceurs couperaient l'herbe sous le pied des malfaiteurs. Un changement de standards qui prendra du temps même si le secteur prend à bras le corps le problème de la fraude publicitaire, comme en témoigne la nouvelle norme mise en place par Adjust, la validation des clics par preuve d'impression. L'écosystème a tout à y gagner : plus sain, il sera aussi plus fiable économiquement !

Maddyness, partenaire média d'Adjust.
