O IAB Brasil (Interactive Advertising Bureau) é uma entidade presente em 45 países com a missão de promover o marketing e a publicidade digital.

Aqui no Brasil, representa mais de 250 associados, entre eles agências, anunciantes, veículos e empresas de tecnologias e serviços.

O objetivo primário do IAB Brasil é a contribuição ao desenvolvimento do mercado digital, incentivando e orientando a criação de boas práticas para o planejamento, criação, compra, venda, veiculação e mensuração de ações publicitárias interativas.

Entre no site www.iabbrasil.net para acessar conteúdos, guias, agenda de eventos, cursos e muito mais.

Participe do IAB e faça parte da construção do mercado de marketing digital brasileiro.

iab. brasil

BOAS PRÁTICAS NO COMBATE À FRAUDE

PARA *PUBLISHERS*

INTRODUÇÃO

O mercado de publicidade digital no Brasil aumenta a cada ano: entre 2016 e 2017, registrou um crescimento de 25,4%, segundo levantamento do IAB Brasil. Esse aumento é essencial para dar espaço a novas tecnologias, produtos e soluções que, por sua vez, contribuem para a manutenção desse avanço. Ao mesmo tempo que o desenvolvimento cria grandes oportunidades para todos, ele também torna o mercado mais complexo, e não se atualizar pode abrir espaço para um grande problema: a fraude.

Em 2017 foi lançado um estudo da TAG* (*Trustworthy Accountability Group*) que verificou que sites fraudulentos lucraram cerca de 111 milhões de dólares apenas no mercado americano. A ANA (*Association of National Advertisers*) estima** que, em 2017, o tráfego em fontes não-humanas, os *bots*, pode ter representado 6.5 bilhões de dólares no mercado global. O Brasil, sendo um importante mercado de publicidade digital, é um grande atrativo para os fraudadores.*** Todos esses valores somam investimentos e esforços de mídia perdidos para agentes fraudulentos. Perdas que não só diminuem os resultados do mercado, mas também enfraquecem a confiança dos anunciantes e a indústria como um todo.

Apesar do volume, a fraude na publicidade online vem mostrando uma retração importante. Essa diminuição é resultado de ações no mercado global, guiados por importantes iniciativas de organizações como o IAB, a TAG e o MRC (*Media Rating Council*).

É no intuito de conscientizar e inspirar o mercado a participar dos esforços contra a fraude que o IAB Brasil construiu o Guia de Combate à Fraude para *Publishers*.

* https://www.tagtoday.net/piracy/measuringdigitaladrevenuetoinfringingsites
** http://www.ana.net/content/show/id/botfraud-2017
*** https://digiday.com/marketing/global-state-ad-fraud-4-charts/ - Acesso em 22/05

TIPOS DE FRAUDE

TRÁFEGO INVÁLIDO GERAL (GENERAL INVALID TRAFFIC – GIVT)

De natureza mais simples, o tráfego inválido geral é diagnosticado mais facilmente por meio de verificações rotineiras e bloqueio de agentes fraudulentos já conhecidos. Dentro dessa classificação, podemos destacar:

Tráfego de Data-centers
É entendido como tráfego de data-centers qualquer tráfego que tenha seu ponto de origem em um data-center ou servidor. Nesses casos o tráfego não foi originado legitimamente por um humano e não deve ser considerado como válido.

Tráfego Automatizado
Os bots, spiders e *crawlers* são tecnologias criadas para simular interações humanas em sites. O tráfego gerado por eles, portanto, deve ser desconsiderado.

Atividades e Navegação Suspeita
Um usuário se comporta de maneira imprevisível, mas com padrões naturais de interação com conteúdo. Qualquer ação suspeita, como preenchimentos de formulário, cliques ou mesmo compras repetitivas, deve ser alertada e filtrada como tráfego inválido.

Tráfego por Ferramentas Incomuns
É importante lembrar que o pré-carregamento utilizado pelos navegadores pode gerar uma impressão antes da efetiva visualização do usuário e, por isso, essa impressão deve ser desconsiderada. O mesmo deve ser feito para qualquer atividade proveniente de um navegador fora do padrão ou não identificado.

TRÁFEGO INVÁLIDO SOFISTICADO (SOPHISTICATED INVALID TRAFFIC – SIVT)

Diferente do GIVT, o tráfego inválido sofisticado é mais avançado e complexo. Filtros de rotina e ações padronizadas não são o suficiente para identificá-lo. Esse processo requer análises avançadas e uma ação humana significativa, com colaboração em diferentes frentes.

Tráfego Automatizado Sofisticado

Os *bots* mais complexos podem assumir cookies de usuários para representar um perfil específico, imitar uma navegação legítima com cliques, interações com o conteúdo e, até mesmo, preenchimento de formulários.

Malware e aparelhos infectados

Os *malwares* podem infectar aparelhos de diferentes formas e, assim, usá-los para gerar tráfego ilegítimo em sites e aplicativos.

Sobreposição de anúncios e anúncios não visíveis (*Ad Stuffing*)

O *ad stuffing* é a sobreposição de diversos anúncios escondidos, multiplicando o número de anúncios entregues quando, na verdade, apenas um deles é visto efetivamente pelo usuário na página. Os anúncios também podem ser colocados atrás de conteúdos da página, fora da área visível da tela ou até mesmo em *pixels* 1x1.

Falsificação de sites

A falsificação de sites ou *Domain Spoofing* é o ato de mascarar um site falsificando um domínio legítimo, com o propósito de roubar o investimento direcionado ao site imitado.

Falsificação de métricas, geolocalização e *cookies*

A manipulação ou falsificação de métricas do site, localização da entrega de anúncios e *cookies*/dados de navegação são todas atividades fraudulentas.

Este material tem como base o guia do IAB de *Boas Práticas no Combate à Fraude 2017*.

BOAS PRÁTICAS PARA *PUBLISHERS*

Os *publishers*, assim como os demais atores da cadeia de publicidade digital, têm um papel fundamental na implementação de regras e processos de combate à fraude. O objetivo desta seção é fornecer boas práticas que podem facilitar a tarefa de detecção de fraudes e contribuir para um ecossistema mais saudável.

CUIDE DE SEU INVENTÁRIO

Antes de tudo, é fundamental para o *publisher* assegurar a qualidade do seu inventário e proporcionar transparência a seus clientes. Algumas dicas básicas são:

- Entenda o volume de audiência disponível e planeje sua entrega;
- Monitore os padrões de tráfego em tempo real, e não só posteriormente;
- Avalie métricas em conjunto e não isoladamente;
- Entenda o KPI de cada campanha. Acompanhe e otimize seu desempenho;
- Implemente iniciativas de transparência da indústria, como o ads.txt.
- Considere a possibilidade de testar o inventário do parceiro por meio de um terceiro (validação de campanhas).

COMPRAR TRÁFEGO AUMENTA SEU RISCO

Muitas vezes, o *publisher* não tem o inventário ou a audiência para entregar o volume contratado. Nesses casos, a compra de tráfego costuma ser uma alternativa. Mas cuidado: isso pode aumentar seu perfil de risco.

A recomendação da TAG é que os *publishers* evitem comprar tráfego, porque isso pode colocar sua reputação em xeque. Mas se, por alguma razão, você precisar aumentar inventário, **não compre de fontes não-orgânicas**, isto é, não utilize técnicas que geram tráfego sem o desejo ou interesse da audiência.

Caso tenha que comprar tráfego, as seguintes dicas podem ajudar a minimizar riscos:

- Priorize a qualidade em detrimento do preço;
- Busque uma afinidade natural entre conteúdo e audiência;
- Use tecnologia para detectar tráfego inválido;
- Conheça seus fornecedores e onde eles compram tráfego;
- Exija o comprometimento de seu parceiro com práticas antifraude.

CONHEÇA SEUS FORNECEDORES DE TRÁFEGO

Coloque-se no lugar do seu cliente. As perguntas abaixo são praticamente as mesmas que anunciantes deveriam fazer aos *publishers*:

- Sua audiência pode ser avaliada por parceiros independentes e confiáveis?
- Você tem uma "ficha limpa" junto a esses parceiros?
- Como você determina quais impressões serão mostradas a usuários reais?
- Como você garante que os anúncios são servidos conforme reportados, e que as URLs estão visíveis para o anunciante?
- Como você determina se os anúncios são iniciados automaticamente ou iniciados pelo usuário?
- Você oferece proteção contra *malware*?
- As impressões geradas por *malware* são redirecionadas para algum site?

IDENTIFIQUE ATORES MALICIOSOS

Operadores de *botnets* (redes de computadores geralmente associadas ao uso de *software* malicioso) e maus atores em geral sempre procuram atuar silenciosamente. Por isso, é importante ficar atento aos seguintes sinais:

- O *publisher* que não tem histórico de tráfego significativo;
- Perfis de audiência muito similares em sites muito díspares;
- Estatísticas de navegação inconsistentes com índices conhecidos (ex.: dados demográficos);
- *Publisher* procurando excessivamente obter representação;
- Excesso de anúncios por página.

COLABORE COM SEUS PARES

Relações colaborativas na indústria formam um muro de resistência que ajuda a afastar atores maliciosos.

- Forme parcerias para compartilhamento de informação com outros elementos da cadeia, como exchanges e DSPs;
- Alie-se a companhias especializadas em combater fraude e *malware*. Isso estabelece uma camada adicional de segurança para o tráfego que você adquiriu.

CRIE SUAS PRÓPRIAS DEFESAS

Defender-se dos maus atores contribui enormemente para aumentar o valor da sua network. Eis alguns métodos:

- Estabeleça "desincentivos" para os times que estabelecem as parcerias. Novas fontes de tráfego devem ser avaliadas por critérios técnicos previamente estabelecidos. Estimule-os a buscar tráfego humano de maior qualidade;
- Monitore todo tráfego suspeito. Se identificado como sendo proveniente de uma fonte fraudulenta, bloqueie-o imediatamente;
- Bloquear tráfego fraudulento na origem consequentemente evita o pagamento a maus atores. Fraudadores terão dificuldade em provar que seu tráfego é válido.

Este material tem como base o guia do IAB de *Boas Práticas no Combate à Fraude 2017*.

CONCLUSÃO

A fraude na publicidade online é uma realidade e afeta seriamente a todos.

Portanto, esse material surgiu com o propósito de estender a conscientização e esclarecimento não só a anunciantes e networks, mas a todos os participantes da cadeia no mercado nacional.

Combater a fraude requer persistência na adoção de boas práticas e uma contínua busca por informação.

Não deixe de visitar o site da TAG e do IAB Brasil para atualizações acerca do tema. A atuação conjunta no combate à fraude traz grandes resultados para todos, inviabilizando o lucro de fraudadores, tornando relações mais transparentes, seguras e valorizando nosso mercado.

O IAB Brasil agradece aos associados membros do comitê de Combate à Fraude em 2018 e, em especial, à presidente do comitê, Luciana Burger, e aos profissionais que compuseram o grupo de trabalho que se dedicou para a produção deste material:

Lucas Vianna, Ad Solutions na Vivo Ads & Terra;
Roberto Gutierrez, Head of Trust & Safety LatAm no Google.