



BOAS PRÁTICAS NO COMBATE À FRAUDE

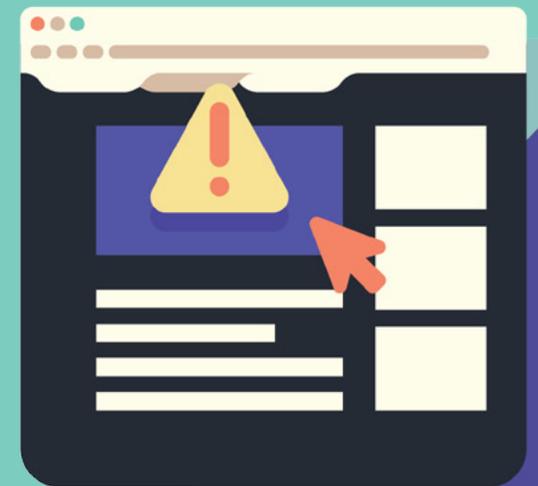
O IAB Brasil (*Interactive Advertising Bureau*) é uma entidade presente em 45 países com a missão de promover o marketing e a publicidade digital.

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.

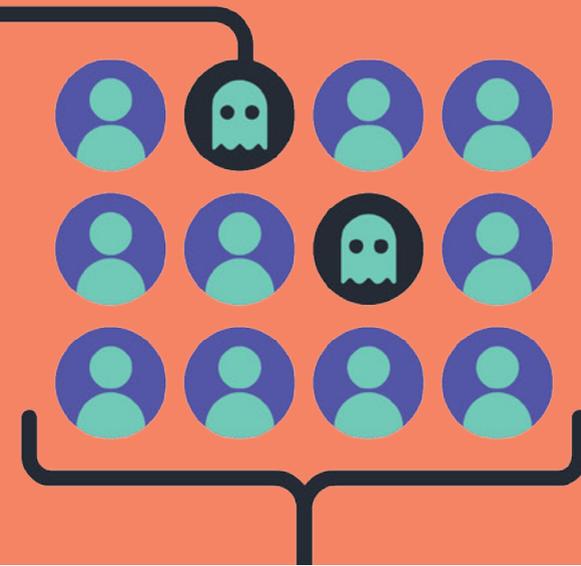
Entre no site www.iabbrasil.net para acessar conteúdos, guias, agenda de eventos, cursos e muito mais.

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





INTRODUÇÃO



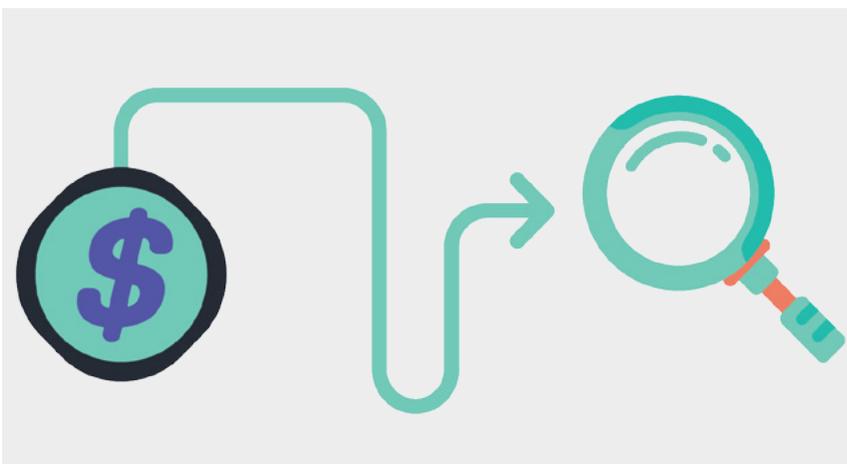
Levantando a bandeira da transparência, o IAB Brasil traz, com prioridade, a questão de fraude na indústria de publicidade online. Para isso, criamos o comitê de combate à fraude. Seu objetivo é educar o ecossistema sobre o assunto e trazer boas práticas, já estabelecidas nos EUA, ao mercado brasileiro.

Podemos definir fraude como uma vantagem ilícita ou de má-fé que visa a ganhos pessoais. No Brasil, encontramos, em nosso dia a dia, diferentes ações criminosas, que se aproveitam e subtraem valores da sociedade. Como exemplo dessas ações, já combatemos fraudes de cartão de crédito em caixas eletrônicos, sites de e-commerce e os que simulam internet banking, objetivando o roubo de senhas. Situações que eram um grande problema para diversos segmentos foram minimizadas por meio da disseminação de conhecimento e boas práticas. Isso já acontece de forma relevante e silenciosa, com verbas publicitárias digitais em todo o mundo. Quando há entendimento do problema, as fraudes diminuem.

A atividade fraudulenta pode ser definida como a prática deliberada de tentar servir anúncios que não têm potencial para serem vistos por um usuário humano, o que normalmente é realizado por meio da utilização de bots (“robôs”). Considerando a complexidade característica da publicidade online, sendo um mercado ainda em evolução e com crescimento exponencial, este guia se propõe a ser a primeira ferramenta do IAB Brasil, baseada em documentos do IAB USA e da TAG (*Trustworthy Accountability Group*) com recomendações globais, que orientará e educará o mercado brasileiro a respeito da fraude em publicidade online.

A TAG é uma associação formada em 2015 unindo os interesses do IAB USA, da 4A's (*American Association of Advertising*) e da ANA (*Association of National Advertisers*), associações representativas dos veículos, anunciantes, agências e empresas de tecnologia que têm a missão de criar transparência nos relacionamentos comerciais e nas transações da indústria de

publicidade digital. Saiba mais do trabalho no site da TAG (tagtoday.net). Estudos concretos do mercado norte-americano estimam perdas entre 6 e 8 bilhões de dólares por ano*, que seriam equivalentes a aproximadamente um terço do mercado de publicidade digital. São bilhões de dólares investidos em publicidades que nunca tornaram “públicas” as mensagens desejadas porque não atingiram pessoas ou não foram vistas. Essas diversas fraudes estão diminuindo os resultados dos anunciantes, removendo postos de trabalho e limitando a capacidade de os veículos se remunerarem. Anunciantes, agências, plataformas, fornecedores e veículos devem estar envolvidos no combate à fraude. A ação mais importante e fundamental que precisamos fazer é entender como a fraude acontece e como ela afeta a publicidade digital.



**The Bot Baseline: Fraud in Digital Advertising* (Estudo do mercado norte-americano). Disponível em: <<http://www.ana.net/content/show/id/botfraud-2016>>. Acesso em 26/08/2016

COMO A FRAUDE FUNCIONA

As fraudes são complexas e estão em constante atualização e mutação de técnicas. A fraude tenta sempre simular o comportamento humano para que não seja detectada. O MRC (*Media Rating Council*) publicou, em outubro de 2015**, boas práticas para reportar tráfego inválido. Seguem alguns exemplos ilustrativos e não exaustivos das categorias atuais.

TRÁFEGO INVÁLIDO GERAL (GENERAL INVALID TRAFFIC – GIVT)

São tráfegos identificados por meio de filtragem de rotina, executados com listas ou outros parâmetros padronizados. Os principais exemplos de filtragem de rotina a partir de listas são:

Tráfego de Datacenters

Tráfego não residencial e nem corporativo que normalmente não é humano. Pode ser filtrado a partir de listas de endereços conhecidos por serem uma fonte consistente de tráfego.

Tráfego Automatizado

Tráfego gerado por programas como spiders, robots e outros *crawlers*, como mecanismos de busca e indexadores de preço, pode ser filtrado a partir de listas de bots conhecidos.

Tráfego de Ferramentas Incomuns

Tráfego gerado por acessos que não foram feitos por um navegador padrão. Pode ser filtrado a partir de listas de navegadores conhecidos.

TRÁFEGO INVÁLIDO SOFISTICADO (SOPHISTICATED INVALID TRAFFIC – SIVT)

É mais difícil de ser identificado. São cenários que requerem ações como análises avançadas, colaboração em várias etapas e intervenção humana significativa para poderem ser identificados como fraudulentos. Alguns exemplos são:

***Invalid traffic detection and filtration guidelines addendum. Disponível em: <[http://mediaratingcouncil.org/101515_IVT%20Addendum%20FINAL%20\(Vers%201.0\).pdf](http://mediaratingcouncil.org/101515_IVT%20Addendum%20FINAL%20(Vers%201.0).pdf)>. Acesso em 23/09/2016*

Bots sofisticados

Dispositivos como celulares e computadores são contaminados com bots ao clicar em links de e-mails fraudulentos ou após instalar programas de sites fraudulentos. Os bots fazem requisições de anúncios sem o controle ou consentimento do usuário e tentam simular o comportamento humano. Podem gerar impressões, cliques, viewability e até preencher cadastros.

Ad Stuffing

Na maioria das vezes, o anúncio não está visível e não pode ser clicado. Os anúncios são intencionalmente escondidos, empilhados ou encobertos com a intenção de inflar os números. Uma indicação da existência desse tipo de fraude é uma taxa de cliques muito abaixo do normal.

Alguns exemplos são fraudes de pixel stuffing, quando um ou mais anúncios, ou até mesmo um site inteiro, são escondidos em um ponto da tela, podendo ser um pixel de 1x1, e fraudes de ad stacking, quando vários anúncios são sobrepostos de modo que apenas o de cima seja visível.





COMO A FRAUDE DE TRÁFEGO (ROBÔS) INFECTA SITES CONFIÁVEIS?

- Induz os consumidores a instalarem barras de ferramentas em seus browsers;
- Aplica a simulação de jogos ou leitores de vídeo em um navegador alternativo;
- Empacota aplicativos escondidos com softwares que podem ser baixados da internet;
- Insere trechos de códigos não detectados no site de diversos veículos;
- Com códigos maliciosos, explora os sistemas operacionais e as vulnerabilidades de segurança do navegador, instalando clandestinamente códigos de tráfego fraudulento;
- Usa páginas de internet com a aparência semelhante à original, mas que, na realidade, são falsas.

BOAS PRÁTICAS RECOMENDADAS

O caminho para eliminar o tráfego fraudulento deve ser constante, considerando que novos tipos de fraude são criados todos os dias. As boas práticas a seguir ajudarão compradores e vendedores a negociarem publicidade online de qualidade, identificando e minimizando a fraude.

BOAS PRÁTICAS PARA BUYERS (“COMPRADORES”)



Estabeleça metas

Definir metas antes de comprar mídia é geralmente uma boa prática. Algumas recomendações específicas na compra de mídia digital estão listadas abaixo:

- Liste objetivos específicos de sua campanha de mídia. Não deixe metas amplas e abertas a diversas interpretações;
- Documente suas metas claramente e obtenha o consentimento de seus parceiros de mídia;
- Esteja disposto a pagar o preço real aos meios de comunicação que você deseja contratar. Por exemplo, o vídeo pre-roll, direcionado a um público específico, com uma audiência engajada, custará mais caro do que um vídeo sem segmentação;
- Não otimize suas campanhas apenas pelo custo.



Tenha relações comerciais boas e transparentes

Os primeiros passos são: exigir transparência de seus fornecedores, conhecer onde a entrega da publicidade é efetuada, saber como tais espaços são comprados e verificar se há garantias para as especificações oferecidas. Em parceria com seus fornecedores, o claro entendimento das razões para potenciais variações pode contribuir para que as expectativas sejam gerenciadas, e as responsabilidades, definidas.



Siga seu dinheiro (follow your money)

Entenda o caminho de seu investimento e como ele é utilizado. Quanto e como cada fornecedor é remunerado? “Onde e como suas peças são veiculadas?” e outras perguntas podem significar a diferença entre uma posição de destaque de sua marca e resultados não atingidos.



Monitore mais de uma métrica

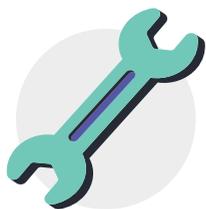
Além do *KPI* contratado, outras métricas devem ser avaliadas para que potenciais riscos sejam evitados. Lembre-se de que bots não se comportam da mesma forma que os seres humanos.

Considere sempre medir os resultados da campanha por meio de um conjunto de métricas. Quando são associadas, as métricas resultam em um método mais sofisticado que reduz a incidência de fraude. A avaliação isolada de métricas, como número de impressões, cliques, CTR (*Click-Through Rate*), percentual de exibição de vídeos (*video completion rate*) e *viewability*, pode ser insuficiente para a detecção de fraudes.



Estabeleça o próprio benchmark

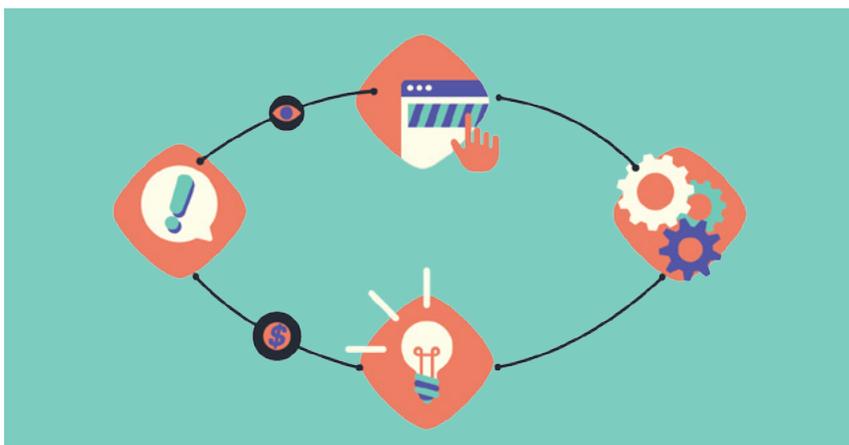
Benchmarks podem ser necessários em suas campanhas. Entenda como as práticas atuais, empregadas por sua empresa e fornecedores, podem ser aplicadas como parâmetros médios de referência.



Conheça as ferramentas disponíveis

Compare as metodologias e ferramentas que podem adicionar valor a seu negócio. Reduzir o risco de exposição significa entender o que se deve monitorar. Além das metodologias, entender os interesses de cada fornecedor é fundamental para estabelecer critérios de avaliação isentos.

BOAS PRÁTICAS PARA SELLERS (“VENDEDORES”)



Muitas vezes, quem vende publicidade não tem o inventário ou a audiência para entregar o volume contratado, o que não representa fraude em si, pois eles podem aumentar sua audiência de forma legítima. A compra de tráfego ou audiência pode aumentar o perfil de risco de um seller. Existem formas diferentes de aumentar a audiência:

NATURAL: as pessoas chegam a seu site de forma genuína (exemplos: anúncios de divulgação de seu site, parcerias de conteúdo etc.);

INDUZIDA: técnicas que carregam o site sem o desejo ou o interesse da audiência (exemplos: pop under, sites carregando de forma involuntária etc.).

A recomendação da TAG é que os publishers evitem comprar tráfego porque coloca sua reputação a longo prazo em risco. Caso o seller opte por estender sua audiência e aumentar seu estoque de publicidade, as práticas a seguir diminuem o risco:

- Priorizar a qualidade em detrimento do preço;
- Procurar uma afinidade natural entre conteúdo e audiência;
- Utilizar tecnologia para detectar tráfego inválido;
- Conhecer os fornecedores e onde eles compram tráfego.

Para mais informações sobre a compra de tráfego, sugerimos a leitura do documento que a TAG publicou em seu site (<http://tagtoday.net/wp-content/uploads/TAG-Inventory-Quality-Guidelines.pdf>), cujo assunto é mais detalhado nas páginas 18 e 19.



CONCLUSÃO

Este guia tem a função de orientar o mercado brasileiro sobre as boas práticas no combate à fraude, minimizando, assim, seu impacto na publicidade digital. Todos os participantes da cadeia devem estar envolvidos em práticas responsáveis, pois qualquer um pode ser afetado e se tornar vítimas dos fraudadores.

Em quaisquer boas práticas adotadas, é fundamental permanecer diligente e continuar buscando o conhecimento. Esta é a primeira das diversas ações que o IAB Brasil e o comitê de combate à fraude farão neste e nos próximos anos, uma vez que estamos tratando de um problema em constante transformação.

iab.
brasil

Revisão do guia de boas práticas lançado em outubro de 2016 pelo grupo de trabalho do comitê de combate à fraude composto das seguintes empresas:

Globo.com: Paris Piedade Neto e Rafael Carvalheira

Google: Gabriela Rodas e Roberto Gutierrez

Tomorro\\:\\: Michel Namora

Tremor Vídeo: Rafael Pallarés

TubeMogul: Adriano Hayashi

FONTES E REFERÊNCIAS

Trustworthy Accountability Group (TAG)

<http://www.tagtoday.net>

Media Rating Council (MRC)

<http://mediaratingcouncil.org/>

IAB USA

<http://www.iab.com/news/iab-releases-final-best-practices-for-reducing-riskof-traffic-fraud/>

PRODUZIDO POR:

Globo.com: Paris Piedade Neto e Rafael Carvalheira

Google: Gabriela Rodas e Roberto Gutierrez

Tempest: Rafael Palermo de Araújo

Tomorro\\:\\: Michel Namora

Tremor Vídeo: Rafael Pallarés

TubeMogul: Adriano Hayashi