Compêndio sobre fraude publicitária para investidores em media

Coautoria da WFA
e THE ADVERTISING FRAUD COUNCIL

Mikko Kotila
Responsável, botlab.io
mailme@mikkokotila.com

Ruben Cuevas Rumin
Professor Assistente, UC3M
rcuevas@it.uc3m.es

Shailin Dhar
Consultor Independente
em Fraude Publicitária
adtechexpert@gmail.com

apan

WFA WORLD FEDERATION OF ADVERTISERS

Compêndio sobre fraude publicitária para investidores em media

CONTEÚDOS

ACERCA DESTE DOCUMENTO

O objetivo deste compêndio é aumentar a consciência dos anunciantes sobre a fraude publicitária e disponibilizar conhecimento e boas práticas para a neutralizar de forma eficaz. Este documento procura encorajar os anunciantes a adotar essas boas práticas e a trabalhar com os parceiros da indústria de forma a fazerem as alterações necessárias para reduzir a fraude de forma substancial.

Este documento foi liderado pelos membros do Global Transparency Group da WFA e aprovado pelos **MEDIA**FORUM e **CDO**FORUM, também da WFA

Por sua vez para a criação, dados e investigação associados a WFA foi apoiada pela Botlab.io, uma fundação de investigação, centrada na investigação da fraude publicitária, na violação dos direitos de utilização e noutras práticas mal intencionadas em toda a cadeia de abastecimento da publicidade online.

Este documento pretende ser apenas um aconselhamento e não um guia definitivo. Tem o propósito da dar uma orientação geral e de elevada qualidade aos associados da WFA e de todas as associações nacionais, como a APAN, sempre que tenham de tomar decisões unilaterais relativamente às suas operações internas e externas nos media digitais.

Publicado em 2016

Compêndio sobre fraude publicitária para investidores em media

SUMÁRIO EXECUTIVO

- Estima-se que a fraude publicitária possa vir a **representar em 2025 cerca de $50 mil milhões, mesmo numa base conservadora. Sem suficientes medidas de defesa é fácil conceber cenários onde as receitas da fraude** publicitária sejam equivalentes a $150 mil milhões por ano, no mesmo prazo.
- Praticamente **toda a compra programática está exposta à fraude publicitária**. Afirmações contrárias devem ser tratadas com cautela.
- Sites de spam viral que oferecem pouca ou nenhuma oportunidade de eficácia publicitárias são endémicos em toda a Internet. Também encontramos fraude publicitária entre os *publishers premium*, por exemplo sob a forma de tráfego originado noutras fontes. **O tráfego originado em fontes de fraca qualidade tornou-se num lugar comum entre os *publishers*, frequentemente como uma forma de entregar *targets* de campanha aos anunciantes.**
- A fraude publicitária tem sido cometida por múltiplos protagonistas. Apesar disso, **o maior benfeitor não intencional da fraude publicitária é a indústria do marketing e da publicidade**.
- Não existe no mercado uma solução definitiva e, na verdade**, uma percentagem mínima de exposição à fraude publicitária irá por certo prevalecer face a quaisquer medidas defensivas.**
- **Os anunciantes são quem perde totalmente com a fraude publicitária** e, a menos que sejam tomadas algumas medidas efetivas, o problema relacionado com esta ameaça continuará a crescer em magnitude e complexidade.
- Até a indústria provar que tem capacidade de lidar de forma eficaz com a fraude publicitária, **os anunciantes deverão ser cautelosos em relação ao aumento dos seus investimentos em media digital**, de forma a limitar a sua exposição à fraude.
- **Muito pode ser feito pelos anunciantes para melhorar a situação,** incluindo o estabelecer novos standards, fazer alterações contratuais, exigir maior transparência, e pôr em prática recursos internos dedicados a neutralizar a fraude publicitária.
- **É exigido à indústria alteração de comportamentos** que só são possíveis de conseguir com uma adequada compreensão do problema, uma motivação comum e uma abordagem partilhada.

"A fraude publicitária é um dos problemas mais importantes que enfrentamos hoje. Estamos empenhados em manter o diálogo de forma a aumentar a consciência e construir soluções. Esperamos que este guia possa conduzir a industria no caminho da identificação de oportunidades e soluções para os anunciantes, publishers e empresas tecnológicas."

Benjamin Jankowski,
Group Head, Global Media
MasterCard & Presidente
do MEDIAFORUM da WFA

Compêndio sobre fraude publicitária para investidores em media

O QUE É A FRAUDE PUBLICITÁRIA?

Por definição a fraude publicitária está associada a uma atividade onde as impressões, cliques, ações ou dados são falsamente reportados para gerarem receitas de forma criminosa, ou para outros fins de fraude ou dolo. As atividades de fraude publicitária destinadas a gerar receita são mais comuns mas, a criação de ruido ou outras atividades que não estejam ligadas à geração de receitas estão atualmente também presentes no ecossistema publicitário da Internet.

Em resumo, existem quarto tipos de esquemas de fraude publicitária:

1. Fraude de impressões
2. Fraude de cliques
3. Fraude de conversão
4. Fraude de dados

Em cada um destes casos o relatório valida a autenticidade de um visitante mas, na verdade ele é fraudulento. Esses visitantes fraudulentos podem ser totalmente mecânicos, humanos ou uma mistura de ambos.

QUAL A DIMENSÃO DA FRAUDE PUBLICITÁRIA?

Com os investigadores a reportar uma exposição à fraude publicitária a níveis tão baixos como 2%[1] e tão elevada como 90%, parece clara a inexistência de grandes formas de identificar a verdadeira taxa de exposição à fraude. O desafio de estabelecer esse valor é sublinhado pelos resultados de uma investigação levada a cabo pela WFA, que demonstra que 36%[2] dos respondentes refere desconhecer até que ponto estão expostos à fraude publicitária. Uma das maiores iniciativas de investigação sobre fraude publicitária foi o recente "Bot Baseline"[3] levado a cabo pela Associação Americana de Anunciantes (ANA). O custo estimado de fraude publicitária foi de $7,2 mil milhões, o equivalente a cerca de 5% do total do investimento em media digital naquele País.

Embora este seja, sem dúvida, um montante extremamente significativo, a investigação preliminar realizada pela Botlab.io em conjunto com os seus parceiros académicos e outras entidades (uma amostra das quais está descrita abaixo), sugerem que a escala do problema pode ser, de fato, muito mais substancial:

- 88% cliques em anúncios digitais são considerados fraudulentos[4]
- os editores digitais conduzem toda a indústria num mau tráfego robotizado em 32%[5]
- os robots inflacionam as audiências comerciais entre 5% a 50%[6]
- o tráfego robotizado é superior a 61.5% de todo o tráfego de websites[7]
- uma única forma de fraude em aplicações representa 13% de todo o inventário das aplicações[8]
- crescimento de 22% num ano de tráfego robotizado fraudulento[9]
- 40% dos cliques em anúncios em telemóveis são absolutamente inúteis[10]
- tráfego de robots aumentou pela primeira vez acima de 50% do total[11]
- mais de 18% das impressões /clicks vêm dos robots[12]

O foco central deste documento não é realizar mais investigação empírica para identificar o montante total que a fraude publicitária representa hoje. Para provocar a mudança na nossa industria é útil, no entanto, conhecer a escala do problema hoje e qual poderá ser a dimensão razoável no futuro, de acordo com diferentes cenários.

Ao longo deste documento têm sido utilizados dois cenários: um relativamente conservador considerando uma taxa de exposição à fraude de 10% e outro com uma taxa mais elevada de 30%. Baseado em estudos realizados por terceiras entidades e um outro preliminar conduzido pela Botlab.io e seus parceiros, fica claro que o verdadeiro valor deverá ser ainda mais elevado do que 30%.

Vale a pena sublinhar que a fraude publicitária não se manifesta apenas sob a forma de tráfego robotizado mas sob outras formas de atividades inválidas (em breve abordadas neste documento), pelo que a taxa de exposição global à fraude será mais elevada do que a quota que o tráfego robotizado representa no total de todo o restante tráfego.

O custo real da fraude publicitária é bastante superior à receita que gera. Um estudo contínuo da Deloitte e da WFA, assim como um trabalho similar levado a cabo pela Advertising Association no Reino Unido[13], mostra que por cada dólar perdido devido à ineficiência publicitária, é gerada uma perca no negócio mais de seis vezes superior. Os tipos de danos causados pela fraude publicitária podem resumir-se a:

1. custo de eficácia de marketing;
2. custo para o negócio (e para toda a categoria do negócio);
3. custo para a economia nacional (e para os contribuintes).

Isto significa que o resultado do ataque à eficácia da publicidade de um determinado anunciante, afeta a economia na qual o anunciante está inserido e para a qual contribui. Desta forma a fraude publicitária representa um novo tipo de risco de segurança, e uma nova maneira de atacar a economia de um determinado país.

"Enquanto anunciantes temos a responsabilidade de combater a fraude publicitária, quer em beneficio dos consumidores que servimos, quer da indústria da comunicação em geral. É importante trabalharmos junto dos nossos pares e parceiros da indústria para resolver os desafios que enfrentamos, e colaborar no sentido de alterar a forma como o atual ecossistema funciona."

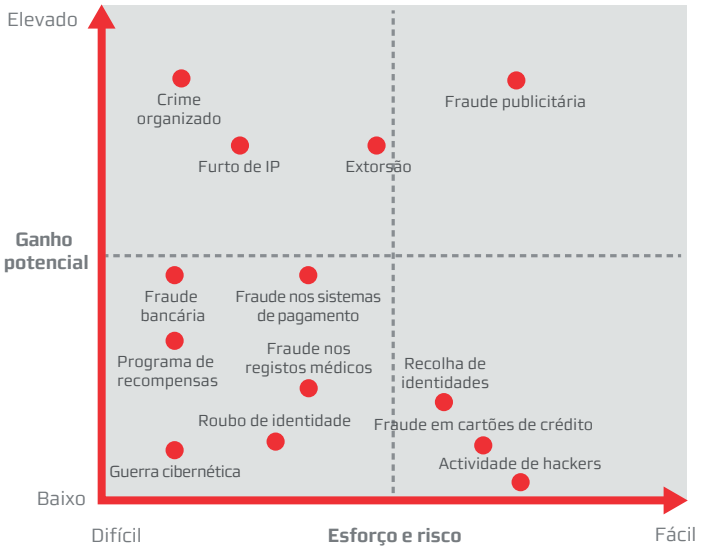
Luis Di Como,
Senior Vice-President, Global Media, Unilever & membro do Global Transparency Group e do Executive Committee da WFA

[1] *Digital Content Next & White Ops > https://digitalcontentnext.org/wp-content/uploads/2015/09/DCN-Bot-Benchmark-Report-2015-.pdf*
[2] *Members only survey Nov. 2015 > http://www.wfanet.org/en/knowledge/global-knowledge-base#/item/314*
[3] *ANA & WhiteOps. The Bot Baseline 2015 > http://www.ana.net/content/show/id/botfraud-2016*
[4] *Oxford BioChronometrics > https://oxford-biochron.com/over-88-of-digital-ad-clicks-deemed-fraudulent-new-study-by-oxford-biochronometrics-suggests/*
[5] *Distil Networks 2015 > http://resources.distilnetworks.com/h/i/155404518-distil-networks-releases-new-data-on-the-state-of-digital-advertising-fraud*
[6] *ANA & White Ops 2014 'The Bot Baseline' > http://www.whiteops.com/botfraud*
[7] *Incapsula Bot Traffic Report 2013 > https://www.incapsula.com/blog/bot-traffic-report-2013.html*
[8] *Incapsula, Mobile app fraud study 2015 > http://www.prnewswire.com/news-releases/forensiq-projects-in-app-ad-fraud-will-surpass-1-billion-in-2015-300117453.html*
[9] *Solve Media 2014 > http://www.businessinsider.in/Botnets-Will-Cause-11-6-Billion-In-Wasted-Ad-Spending-This-Year/articleshow/29508619.cms*
[10] *Trademob 2012 > https://gigaom.com/2012/08/31/report-40-percent-of-mobile-clicks-are-fraud-or-accidents/*
[11] *Solve Media 2013 > http://www.adweek.com/news/advertising-branding/bot-problem-keeps-getting-worse-154585*
[12] *Bin Liu, University of Southern Calfornia 2014 > https://www.usenix.org/node/179764*
[13] *Deloitte & Advertising Association (UK) 2011 > http://www.adassoc.org.uk/publications/advertising-pays/*

O QUE NOS RESERVA O FUTURO?

A digitalização, o cibercrime e as tendências de fraude publicitária são os principais impulsionadores para o crescimento da fraude publicitária nos próximos 10 anos. A menos que aumente a capacidade de contra-atacar a fraude publicitária paralelamente ao montante do investimento no digital, a taxa de exposição à fraude publicitária aumentará significativamente em termos absolutos.

Há muito poucos casos em que a fraude publicitária levou à acusação[14] e condenação[14], o que significa que o nível de 'risco' é baixo relativamente a outro qualquer crime digital. Um relatório recente da Hewlett Packard classifica a fraude publicitária como tendo um elevado 'ganho potencial' relativamente a qualquer outra forma de crime digital[15]. Prevê-se que a combinação destes fatores atraia 'spammers', organizações de crime e outros criminosos que anteriormente poderiam ter estado centrados em áreas alternativas.



Fonte: Hewlett Packard Enterprises, 'The Business of Hacking', Maio 2016

Quanto mais tempo for permitida a duração da fraude publicitária, mais difícil se torna combatê-la.

Estima-se que em 2025 o total do investimento em todo o mundo será da ordem dos $400-$500 mil milhões[16]. Se apenas 10% do limite superior deste intervalo estiver exposto à fraude publicitária, esta será simplesmente a segunda forma de crime organizado[17] logo após a cocaína e os opiáceos.

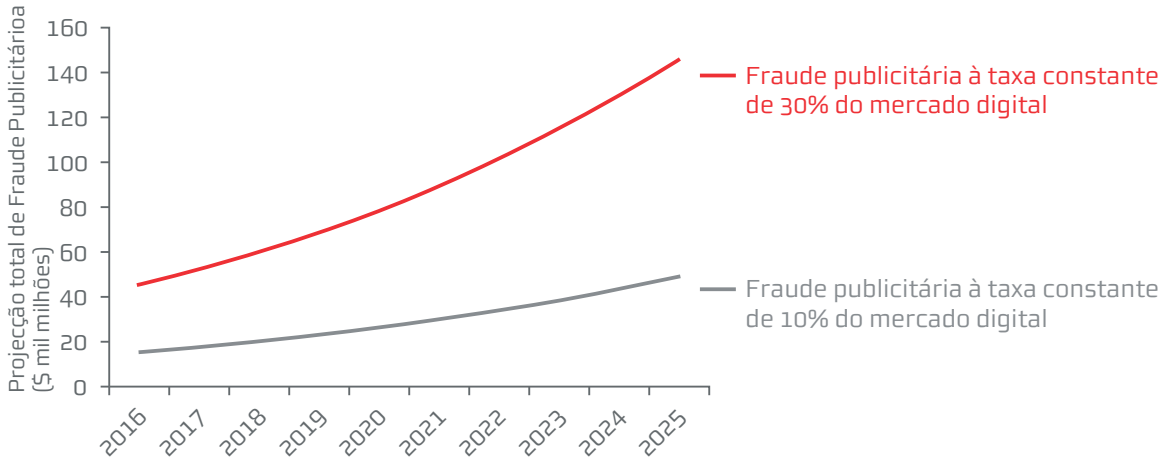
Contudo, como ilustrado anteriormente, investigações recentes referem que a fraude publicitária representa bastante mais do que 10% do mercado digital. Na verdade, ela pode representar já bastante mais do que 30% - o cenário mais grave que referimos ao longo deste documento.

Simples matemática mostra que 30% de $150 mill milhões em 2016, representariam $45 mil milhões. Assumindo que este valor se manteria constante nos próximos 9 anos, então, apenas o crescimento resultante do aumento do mercado publicitário digital representará $140 mil milhões em 2025.

[14] *Notably, the FBI's expose of fraud conducted by affiliate marketers (http://uk.businessinsider.com/ebay-the-fbi-shawn-hogan-and-brian-dunning-2013-4?r=US&IR=T) and the sentencing in the US of an individual for click fraud (http://www.reuters.com/article/us-usa-cybersecurity-malware-idUSKCN0XN2WX)*
[15] *Hewlett Packard Enterprises, 'The Business of Hacking', May 2016*
[16] *Based on historical trends from GroupM and ZenithOptimedia, plus WFA projections based on future market forces.*
[17] *https://www.unodc.org/toc/en/crimes/organized-crime.html*

Claro que é altamente improvável que a fraude publicitária não cresça para além de sua base atual, já que a verdade é que ela cresceu rapidamente, à medida que os seus responsáveis aumentaram em sofisticação. Embora se possa discutir a possibilidade de uma taxa de exposição à fraude ser de 10%, 30% ou maior ser correta, será difícil contestar que há um forte elemento de conservadorismo colocado nas projeções abaixo.

A menos que aconteçam alterações dramáticas no ecossistema tecnológico da publicidade e na forma como o dinheiro está a ser investido em media pelos anunciantes e parceiros da indústria, o valor mais baixo de $50 mil milhões em 2025 ilustrado no gráfico abaixo, pode em breve parecer mais um valor impossivelmente baixo do que uma estimativa conservadora



Fonte: Projeções da indústria baseadas no crescimento do mercado de media digital e cenários possíveis do crescimento da fraude publicitária

Conclusões da investigação da WFA identificam que 9 em cada 10 (92%) dos anunciantes respondentes concordam que a fraude publicitária é perpetrada pela estrutura e sistemas do ecossistema de media digital. Compete ao ecossistema, incluindo editores e outras entidades do lado das vendas, mais as empresas de compra programática, agências e outras empresas do lado da procura, provar a capacidade de lidar eficazmente com a fraude publicitária. **Até lá, os anunciantes devem ser cautelosos em relação aos seus investimentos na totalidade dos media digitais, limitando o crescimento e a exposição à fraude publicitária.**

"O crescente investimento no digital tem oferecido tantas oportunidades quantos desafios, mas poucos são tão prementes quanto este. Precisamos pôr em funcionamento as medidas apropriadas para proteger as nossas marcas e os nossos clientes. Há muito a aprender do setor financeiro que continua a combater a fraude online"

Mark Butterfield,
Head of Global Media,
Boehringer Ingelheim Ltd
& membro do Global
Transparency Group
da WFA

QUE FORMAS ASSUME A FRAUDE PUBLICITÁRIA?

Existem três formas básicas de fraude publicitária:

1. Site. Podem ser divididos em sites que estão sob o controle do perpetrador[19], e naqueles em que o perpetrador atua como associado, como é tipicamente o caso dos esquemas de fraude de conversão.

2. Plataforma. Pode ser qualquer coisa a partir de um site de rede social para um site de alojamento de vídeo. No caso das marcas estarem mais familiarizadas com as plataformas, inevitavelmente, há uma maior confiança e menores suspeitas de fraude. Há evidências de que as principais plataformas têm problemas significativos de fraude publicitária[20].

3. *Data*. Refere-se às circunstâncias em que os inimigos são capazes de rentabilizar dados do utilizador através do mercado de dados. Existem várias maneiras de o executar virtualmente, mas um exemplo é através do envio de um robot da internet (*botnet*) a visitar sites de editores, tornando-se esse robot parte daquilo que o editor consideraria ser *first party data*. Muitos editores utilizam *cookies* para localizar audiências e vender anúncios em sites que não são deles, utilizando técnicas de extensão de audiências e, dessa maneira propagarem falsas impressões em toda a web. Passos adicionais incluem o envio de robots a visitar sites de anunciantes, qualificar os *cookies* como *first party data* do anunciante e deixar os dados da marca envenenados[21].

Qualquer comprador de programático poderá estar virtualmente exposto a fraude publicitária; mesmo as compras programáticas diretas de TV são vulneráveis. Quaisquer alegações do contrário devem ser tratadas com precaução.

No caso da fraude em sites, a forma mais antiga e mais comum de fraude publicitária utilizada, há três aspetos chave a considerar.

1. Spam-sites. Este é um fenómeno (abordado em detalhe abaixo) unicamente associado à fraude publicitária. Apesar de existirem grandes recursos disponíveis para análise e criação de listas negras de endereços de IP associados ao tráfego fraudulento, não existem disponíveis esses mesmos recursos para a fraude publicitária relacionada com sites de spam. Dos top 5.000 sites de tráfego disponíveis aos compradores de media através do mercado digital de anúncios, quase 30% utiliza soluções de privacidade que tornam difícil, ou virtualmente impossível, ligar um site a um indivíduo ou empresa.

   Estes sites tipicamente enviam 10 a 100 vezes mais tráfego para o mercado de anúncios digital do que sites como o Alexa[22] sugerem ser possíveis. Não é invulgar para esses sites enviarem, num único dia, centenas de milhares de impressões (ou mais) para serem vendidos no mercado de compra de anúncios digitais.

2. Tráfego. É importante perceber que existem dois tipos de tráfego; um com potencial de eficácia publicitária e outro sem potencial de eficácia publicitária. Exemplos do tipo de tráfego que caem nesta última categoria incluem:

   - *auto-refresh traffic* – quando os motores de busca dos utilizadores estão permanentemente a atualizar a página (ou os anúncios da página)
   - *clickjacking traffic* – quando um utilizador é "forçado" a clicar em algo mais do que pensa que está a clicar[23]
   - *cloudbot traffic* – tráfego proveniente de endereços de IP hospedados na nuvem da empresa[24]
   - *common botnet traffic* – tráfego proveniente de dispositivos de utilizadores pouco seguros
   - *cookie stuffing traffic* – redireccionamento de um utilizador para um site com o propósito de colocar um *cookie* associado no motor de busca[25]
   - *farm traffic* – ações do utilizador (normalmente conversões), repetidas por um grande número de pessoas[26]
   - *hidden ads* – anúncios "empilhados" em cima uns dos outros, ou escondidos do utilizador de outra forma
   - *social spam traffic* – links enganosos postadas nas redes sociais que resultam em visitas sem valor

3. Robots de spam. Um robot típico das redes sociais pode colocar conteúdos de múltiplos sites centenas de vezes por dia. Estes *robots de spam* das redes sociais são utilizados para criar a impressão de um site popular, mostrando elevados níveis de partilha associadas ao conteúdo do site.

Em última análise, é irrelevante se o tráfego ilegítimo resulta de tráfego gerado por robots da internet, uma de várias formas de tráfego mencionados acima, ou por outros meios. O importante é a ausência de potencial de eficácia da publicidade.

O foco da indústria deverá centrar-se nas duas áreas onde o dinheiro da fraude publicitária está a ser gerado; sites de *spam* ou tráfego gerado a partir de *third party data*.

[19] *Digiday/Mike Nolet > http://digiday.com/platforms/one-fraud-site-netted-161-million-impressions-one-week/*
[20] *http://www.ft.com/cms/s/0/53ac3fd0-604e-11e5-a28b-50226830d644.html#axzz49fKzb39V*
[21] *https://medium.com/ad-fraud/direct-buy-poisoning-how-data-fraud-leaves-transactions-vulnerable-to-fraud-a5cc25f11319*
[22] *http://alexa.com*
[23] *https://en.wikipedia.org/wiki/Clickjacking*
[24] *http://www.darkreading.com/cloudbot-a-free-malwareless-alternative-to-traditional-botnets/d/d-id/1297878*
[25] *https://en.wikipedia.org/wiki/Cookie_stuffing*
[26] *https://en.wikipedia.org/wiki/Click_farm*

SITES DE SPAM VIRAL E TRÁFEGO GERADO

A grande maioria dos Top 5,000 sites (de inventário) disponíveis no mercado de publicidade digital são, de alguma forma, sites virais[27]. Esses sites, e inúmeros outros como eles, estão a tomar uma parte substancial do investimento total em media programático, e a qualidade do seu tráfego sugere muito pouco espaço para a eficácia da publicidade do investimento feito.

Os atributos típicos desses sites incluem:

Estes sites competem diretamente com os editores *premium*, por uma quota dos orçamentos de investimento em media, o que pressiona muito esses editores a comprar tráfego gerado por *third party data*. Alguns investigadores consideram a compra de tráfego de fontes terceiras, uma prática generalizada até mesmo entre os editores mais conhecidos.

O tráfego comprado a uma fonte terceira tornou-se, para as publicações digitais, no equivalente às drogas para melhoria de desempenho no desporto; se quiser competir ao mais alto nível, a maneira mais segura de o fazer é através do recurso ao *"doping"*. Semelhante à dopagem no desporto, o tráfego gerado a partir de fonte terceira dá ao editor uma vantagem injusta sobre os que estão "limpos".

O problema é que uma vez iniciado no *"doping"*, torna-se quase impossível parar sem afetar negativamente o desempenho.

Enquanto a identificação de uma taxa de exposição à fraude publicitária credível, quer em termos globais quer locais continua a ser difícil de estabelecer, temos vindo a assistir, durante a monitorização regular de campanhas dos nossos maiores clientes, a editores individuais com 100% de atividade não-humana, e a alguns dos maiores editores (premium) com + 70% de tráfego não-humano. Embora alguns editores se possam envolver diretamente na compra de tráfego através de robots da internet, o tráfego não-humano nos editores premium é principalmente devido à baixa qualidade do tráfego gerado a partir de entidades terceiras, web crawlers e dos scrapers".

Ehsan Mokhtari,
President & Founder of Sentrant Security & Advertising Fraud Council member

O tráfego pode ser adquirido especificamente para atender às exigências dos principais fornecedores de verificação, a um valor bem abaixo dos $0,01 por clique, incluindo empresas de medição de audiência e empresas de combate à fraude publicitária. Também pode ser manipulado para ter a aparência de taxas de visibilidade mais elevadas do que o tráfego legítimo. Considerando que os editores legítimos só podem oferecer o que realmente têm, os autores da fraude publicitária podem ajustar o seu inventário para se tornarem mais desejáveis aos algoritmos de compra, criando uma vantagem sobre os vendedores legítimos em lances vencedores de compras de inventário.

Recomendações aos anunciantes para melhor gerirem, e limitarem, a sua exposição ao tráfego comprado estão documentadas no recente relatório da Associação Nacional de Anunciantes (ANA, US): 'Sourced Traffic: Buyer Beware'. As recomendações incluem o pedido de transparência, o pedido de relatórios das agências, a definição de objetivos de campanha razoáveis e a atenção aos editores mid e long-tail.

Este relatório também se refere ao Publisher Sourcing Disclosure Requirements (PSDR), um conjunto de indicações desenvolvidas pelo Trustworthy Accountability Group (veja mais na pág. 18 abaixo), onde é exigido aos editores que partilhem a quota de tráfego comprado em relação à totalidade da audiência.

Os algoritmos podem também dar prioridade a certos sites de *spam* viral em relação a outros sites, por serem percebidos como oferecendo inventário mais 'desejável'. Isso está ligado ao uso generalizado de troca de segmentação pelas mesas de compra DSP e plataformas de procura, algo facilmente verificável pela investigação do registo de negociações de um determinado (DSP) do anunciante. Um dos fatores de desejabilidade é a capacidade de um determinado editor cumprir qualquer volume de procura. Por causa da pressão a que as mesas de negociação estão sujeitas para cumprir as metas do orçamento, muitas vezes estabelecidos pelos clientes com base noutros critérios de procura, os algoritmos das plataformas de compra podem ser influenciados para a compra de sites de fraca qualidade[28].

Até o regime de compras ser substituído por uma forma mais inteligente de atingir o mesmo objetivo, os site de *spam* vão continuar a capturar uma grande parte do mercado de compra programática, representando agora mais de 200 mil milhões de eventos por dia.

[27] *Botlab.io Media 5k > http://botlab.io/media5k/*
[28] *http://www.minonline.com/news/The-Bots-Have-It-Ad-Fraud-and-Premium-Pubs_26247.html#.VzRM3hUrK7p*

QUEM SÃO OS AUTORES DA FRAUDE PUBLICITÁRIA?

Os principais autores da fraude publicitária são os chamados marketers de 'black hat' - tecnologistas de marketing altamente qualificados. Outros autores incluem as redes de anúncios ilegítimos e cibernautas criminosos.

O envolvimento nesta área do crime organizado ainda é limitado nesta altura, mas isso é suscetível de mudar à medida que os criminosos que têm estado tradicionalmente envolvidos no *spamming* e outras formas de crime cibernético aumentarem o seu envolvimento na fraude publicitária. Para abrandar tal progresso, é necessário um precedente legal nas principais jurisdições de condenações comparáveis a outras formas de cibercrime. Este é um dos fatores-chave de prevenção, o que poderá de outra forma levar a um crescimento dramático da fraude publicitária.

A fraude publicitária é tipicamente levada a cabo pelos seguintes adversários que caem dentro de três distintos grupos, cada um deles com vários graus de níveis de competência e compromisso com esta prática.

	COMPETÊNCIA	COMPROMISSO	AMEAÇA
Adversários do marketing			
Marketers "black hat"	ESPECIALISTA	MUITO ALTO	MODERADO
Certas redes de anúncios ilegítimos	MODERADO	BAIXO	MODERADO
Adversários criminosos			
Criminosos informáticos comuns	MODERADO	BAIXO	BAIXO
Criminosos organizados	MODERADO	ALTO	ALTO

Fonte: Categorias e descrições com base na pesquisa e experiência do Advertising Fraud Council. A ameaça refere-se ao nível de ameaça que o tipo de adversários cria à sociedade.

Marketers "black hat". Muitos dos marketers "back hat" vêm da gestão informática, de um intermediário de marketing ou de alguém com antecedentes de conhecimento avançado de SEO (Search Engine Optimisation). Mesmo como operadores solitários, os marketers "black hat" são capazes de operar em larga escala e normalmente são especialistas de marketing tecnologicamente muito qualificados e com uma profunda compreensão da persuasão e da psicologia das contra-operações..

Certas redes de anúncios ilegais. Sabe-se que existem redes de anúncios ou plataformas de anúncios que participam na atividade de fraude publicitária, muitas vezes agindo como intermediários entre os marketers "black hat" e os que fazem intercâmbio de publicidade. Modelos de desempenho por ação (CPA) são comuns entre estas redes de compra de publicidade. Á primeira vista, algumas destas redes de compras de publicidade, aparecem como totalmente legais e muitas vezes têm acesso aos investimentos em publicidade *premium* quer diretamente das marcas quer das suas agências parceiras.

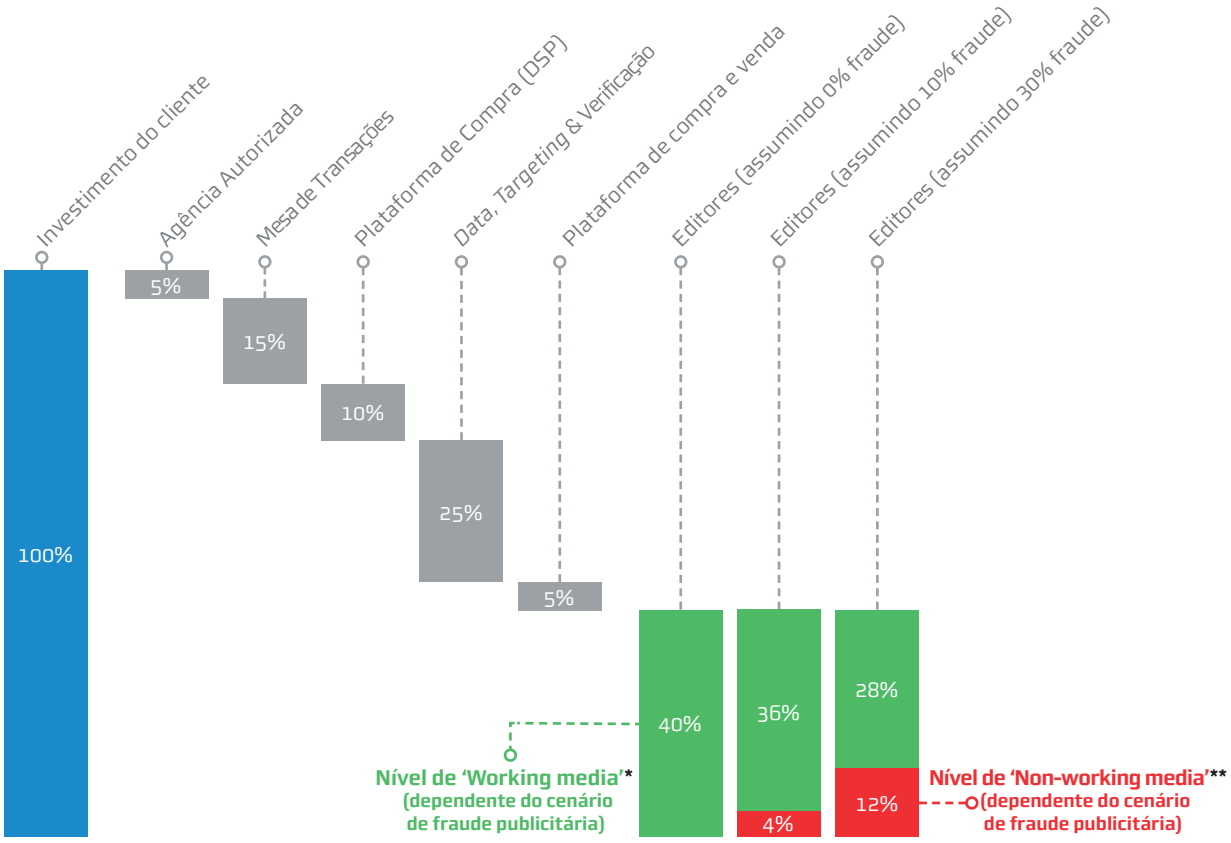
Criminosos informáticos comuns. Com antecedentes no cibercrime, no *spam* e no *phishing*, por exemplo, os criminosos informáticos podem ter sido atraídos pela fraude publicitária devido ao enorme potencial de recompensa disponível.

Crime organizado. É provável que haja um envolvimento significativo de um tipo de criminosos que anteriormente não estavam envolvidos na criminalidade informática. O modelo de crescimento abordado neste documento prevê que, de acordo com a trajetória atual, a fraude publicitária seja em 2015 a segunda forma de crime em receitas, apenas antecedido pela cocaína e opiáceos.

O CIRCUITO DO DINHEIRO NA FRAUDE PUBLICITÁRIA: AVALIAR OS CUSTOS AO LONGO DA CADEIA

Há várias maneiras de os anunciantes comprarem media digital, mas a compra programática é, de longe, aquela que mais rapidamente cresce. Existem muitas razões para isso, nomeadamente as melhorias de desempenho que os anunciantes identificaram nesta forma de compra. No entanto, a complexa infraestrutura tem servido para exacerbar a vulnerabilidade do ecossistema, como referido no Guia de Gestão Programática da WFA lançado pela APAN[29].

Atendendo a que a compra programática tem sido amplamente antecipada como vindo a tornar-se na abordagem universal para a compra de todos os meios de comunicação, foi tomado como base para a análise abaixo uma compra típica em programático. Isto mostra onde é que a fraude publicitária entra no ecossistema e ilustra o impacto que tem sobre o investimento de um anunciante ao longo de todo o processo.



Fonte: Estimativas da indústria

Vários intermediários estão envolvidos na compra programática típica, incluindo as mesas de negociação, as Plataformas de Compra (DSP), os fornecedores de verificação e assim por diante, cada um exigindo uma quota do investimento publicitário.

Aproximadamente 40% do investimento é recebido pelo editor com acesso aos utilizadores do fim da cadeia. O designado 'working media'. Mas a realidade é que uma quota de tráfego é fraudulenta e não tem qualquer potencial de eficácia publicitária.

Após introduzir os cenários de fraude publicitária estabelecidos anteriormente neste documento, os níveis de 'working media' são posteriormente diluídos: para 36% quando se aplica o nível de exposição de 10% e apenas para 28% do 'working media' no cenário de 30% de fraude publicitária.

[29] *WFA Guide to Programmatic Media 2014 > www.wfanet.org/programmatic*
** Valor líquido investido, ** Valor bruto investido (inclui fees de todos os intermediários)*

Antes de o autor da fraude publicitária entrar na cadeia, a indústria 'formal' já foi envolvida e pagou pela sua parte no processo. Este é naturalmente o caso, independentemente do nível de exposição à fraude publicitária e independentemente do facto da rede de anúncios ou do editor serem legítimos ou estarem a operar num esquema de fraude publicitária.

Em ambos os cenários de exposição considerados nesta análise, **o principal benfeitor da fraude publicitária (embora não intencional), é a indústria de marketing. Enquanto 12% das receitas obtidas a partir da fraude publicitária são recebidos pelos autores da fraude no cenário de 30%, os restantes 18% são absorvidos pelo ecossistema legal.**

Não deve ser assumido que, indo diretamente aos editores (programático direto) todo o risco à fraude publicitária é eliminado. Sites de *spam* aparentando serem *premium* prevalecem entre as trocas e até mesmo editores *premium* legais apresentam alguns riscos de fraude publicitária devido ao uso de tráfego comprado (coberto anteriormente neste documento), juntamente com outros fatores.

Por causa dos seus ganhos no ecossistema de media digital, falta a motivação à maioria das empresas de tecnologia de publicidade e plataformas de anúncios para tomarem as medidas necessárias e urgentes para criar um ecossistema de publicidade na internet seguro e transparente. **Como resultado, os custos da fraude publicitária são suportados exclusivamente pelos anunciantes e pelos contribuintes.** Os anunciantes não asseguram a eficácia do seu investimento e, nalgumas circunstâncias os computadores dos consumidores podem ser infetados por vírus com o propósito de cometerem ações fraudulentas, aparentemente por parte do utilizador.

O CIRCUITO DO DINHEIRO NA FRAUDE PUBLICITÁRIA: COMO ACONTECEM AS TRANSAÇÕES

A perpetuação do problema da fraude publicitária está em grande medida ligada às políticas e práticas que outros *stakeholders* têm em relação ao pagamento dos seus parceiros editores. Em muitos casos um grande agregador de inventário ou de transações tem apenas um endereço de e-mail para contactar o parceiro editor a quem paga dezenas ou centenas de euros por mês. Eles podem nunca ter conhecido qualquer pessoa associada ao editor. No entanto, ao longo do tempo milhões de euros poderão ser transacionados desta forma entre as duas partes. Quanto maior for a rede agregadora de inventário, mais difícil é qualquer diligência a este respeito.

Transações de fraude publicitária – onde as compras programáticas são feitas através de um mesa de transações

1. Anunciante paga à agência
2. Agência paga à plataforma de compras (DSP)
3. Plataforma de compras (DSP) paga ao mercado bolsista de anúncios
4. Mercado bolsista paga ao editor (ou a um canal de anúncios em rede que depois paga ao editor)

Todas as transações ocorrem através do sistema bancário formal de acordo com práticas contabilísticas semelhantes à das grandes empresas. **Desta forma, o editor, que pode ser de fato um criminoso informático em larga escala, pode operar como parte da economia formal.**

Não são raras as empresas de fachada, e servem como forma de dissociar ainda mais o adversário da atividade de fraude publicitária em que está envolvido. Estas empresas podem ser constituídas rapidamente e em dimensão. As redes de inventário e as plataformas de anúncios não verificam suficientemente os antecedentes dos seus parceiros, que frequentemente nunca conhecem, por ser muito simples operar sob um uma identidade fabricada, por exemplo uma adquirida no mercado negro de identidades.

Em resumo, quanto maiores forem as legitimas plataformas individuais e centralizadas de anúncios, maior a sua quota na economia da fraude publicitária. Mesmo sem qualquer envolvimento direto nesse tipo de atividade ou sem qualquer intenção de obter ganhos da fraude publicitária

UM GUIA DE COMBATE À FRAUDE PUBLICITÁRIA PARA ANUNCIANTES

A fraude publicitária e os vários aspetos relacionados com ela, e que a causam, são complexos, mas muito pode ser conseguido ao nível de um anunciante individual em termos de resultados de curto prazo. **No entanto, a menos que haja ação da parte dos grandes anunciantes, juntamente com uma abordagem comum e partilhada para resolver o problema, mesmo os ganhos individuais de curto prazo diminuem rapidamente se os problemas estruturais subjacentes à indústria da publicidade continuarem a crescer em magnitude e complexidade.**

Este guia não irá identificar diferentes investigações de combate à fraude publicitária e métodos de análise de dados, nem métodos de deteção ou informação amplamente disponíveis no contexto específico da fraude publicitária. Num mercado de fraude publicitária em rápida mudança, esses métodos utilizados separadamente da orientação que disponibilizamos abaixo, levarão, na melhor das hipóteses, a ganhos individuais de curto prazo e, na pior, a uma maior sofisticação dos adversários.

A única maneira das coisas mudarem é através da alteração de comportamentos. Neste caso, compreendendo, gerindo e efetivamente combatendo a fraude publicitária. Mudança de **comportamentos** é o resultado de **gatilhos** que atuam como lembretes do porquê de um determinado comportamento ser importante que mude; **motivações** que enfatizem a seriedade da necessidade de mudança, e **competências** que permitam que a mudança necessária ocorra.

1. PESSOAS E TECNOLOGIA

Desenvolva recursos internos.

Como todas as soluções de terceiros são de pequenas *startups* ou de empresas que anteriormente faziam outras coisas, **é essencial desenvolver competências internas para apoiar a seleção de fornecedores e outras tomadas de decisão - mesmo que seja apenas uma pessoa dedicada**. Nesta altura não é aconselhável uma dependência exagerada de entidades externas como sejam os fornecedores de verificação. Assim como também não é a dependência da sua agência na condução de atividades de combate à fraude publicitária, uma vez que elas ainda não estão preparadas para o fazer nem são incentivadas a isso.

Incentive fornecedores externos a alavancar soluções abertas.

Uma das chaves do sucesso dos Sistemas de Deteção de Intrusos e da Filtragem de Email Spam (duas das maiores áreas de combate à atividade de cibercrime semelhante à fraude publicitária), é que mesmo os maiores e mais respeitados fornecedores de hoje tendem a usar as mesmas soluções abertas como base das suas ofertas proprietárias. O sucesso alcançado com a segurança na rede (Deteção de Intrusos) e a deteção de *spam* de email, com base em tecnologias comuns e abertas, ilustra a necessidade de uma abordagem semelhante para a fraude publicitária, em oposição a soluções táticas proprietárias. **Soluções proprietárias puras são, na melhor das hipóteses, facilmente reduzidas a melhorias temporárias contra o agressor e, na pior, em melhorias nas competências do agressor.** Onde forem aplicadas soluções proprietárias externas de combate à fraude publicitária, é recomendável que sejam feitos testes regulares por amostragem em paralelo com outras soluções, a fim de monitorizar a fidelidade da tecnologia.

Trabalhe de perto com parceiros de segurança cibernética.

A maioria dos grandes anunciantes já tem consideráveis relações com empresas de segurança cibernética. Estas empresas têm já um histórico na redução sistemática á exposição a problemas semelhantes à fraude publicitária e terão também menos tendência para uma abordagem particular de combate à fraude publicitária. Trabalhar em conjunto com parceiros no campo da segurança cibernética fora da tecnologia publicitária, é uma forma simples de melhorar a compreensão de ameaças comuns relacionadas com a publicidade na internet, e receber avaliações e soluções imparciais de fornecedores de tecnologia de publicidade.

Exija total transparência do seu investimento.

Muito do investimento em media é atualmente, e até certo ponto, opaco ao nível do mercado de troca. **Discussões em torno da transparência devem começar com a disponibilidade de divulgação completa e precisa dos referenciadores (websites), pertencentes a investimentos acima de um determinado nível de inventário.** Outra razão frequente para os anunciantes não terem a divulgação completa sobre como o seu dinheiro é gasto, está ligado à forma como as agências de media reportam o investimento. Insistir na transparência a este nível em todo o ecossistema é uma das formas mais rápidas e seguras de criar bases para um mercado mais seguro.

2. EDUCAÇÃO E COMUNICAÇÃO

Estabeleça expectativas claras.

A revisão dos contratos e incentivos dos parceiros tem de começar com uma clara articulação de expectativas. Por exemplo, não é uma expectativa razoável dizer que não pode haver qualquer fraude, já que isso levará o parceiro a encontrar formas de reportar algo que atualmente é simplesmente impossível. **É muito importante compreender que uma percentagem de exposição à fraude publicitária irá certamente prevalecer contra qualquer medida de combate.** Afirmações de fornecedores em sentido contrário devem ser tratadas com cautela.

Estabeleça métricas apropriadas.

Os parceiros não têm sido suficientemente incentivados a evitar a fraude publicitária – um problema no coração desta epidemia. É importante compreender que **mudar de CPM (Custo por Mil Impressões) para CPC (Custo Por Clique) ou CPA (Custo Por Aquisição) não é solução para reduzir a fraude publicitária – frequentemente torna a situação pior e mais difícil de combater**. As únicas exceções são os casos onde os pagamentos pelos negócios feitos por CPA são baseados nos resultados efetivos no negócio, tal como acontece com um novo cliente de um banco ou com produtos vendidos que não são reembolsáveis. Como exemplo, um banco não obtém qualquer valor de uma aplicação de cartão de crédito resultante de um negócio por CPA, mas sim de um cliente que faz um depósito numa conta aberta ou use o cartão do banco em questão. As métricas de *performance* necessitam, sempre que possível, de estar relacionadas com o resultado efetivo no negócio do anunciante.

Partilha aberta de informação.

Descobertas relacionadas com a fraude publicitária devem ser partilhadas com todas as possíveis entidades homólogas, interna e externamente, em toda a extensão que seja legalmente possível. A fraude publicitária move-se muito facilmente mas é muito difícil de reduzir pelo que, partilhar informação abertamente é a chave do sucesso para todas as partes envolvidas. **O trabalho conjunto e a partilhar aberta é uma das áreas em que a indústria pode ser melhor do que os agressores, que frequentemente trabalham em total isolamento uns dos outros, ou mostram hostilidade uns para com os outros.**

3. STANDARDS

Listas que substituem as compras *run-of-exchange

As compras *run-of-exchange* (ROE) devem ser evitadas. Estas compras, onde os anúncios são comprados às cegas ao longo de milhões de sites, é uma das formas mais certas de alocar dinheiro à fraude publicitária. As compras em ROE beneficiam os fornecedores tecnológicos de publicidade, e não têm qualquer outro benefício. O contra argumento frequente do fornecedor é de que é a única forma de uma plataforma de anúncios atingir os objetivos orçamentados em termos do total gasto por campanha ou por determinado período de tempo. Um argumento que, por si só, indica claramente os problemas estruturais profundos da indústria. No curto prazo, os anunciantes têm de aceitar que, nalguns casos os 'alvos' dos investimentos digitais não serão atingíveis sem expor as compras a elevados níveis de fraude.

** (refere-se a opção de direcionar todo o inventário disponível para o mercado de compra e venda de publicidade).*

"O inventário de publicidade sem qualquer fraude publicitária pode ser impossível de conseguir. No entanto, devemos ser implacáveis. Trabalhando juntos. Aprendendo e partilhando interna e externamente. E através da definição de objetivos progrediremos, pouco a pouco. Estamos a utilizara a mesma abordagem em relação à 'viewability' – e está a funcionar."

Gerhard Louw,
International Media,
Deutsche Telekom AG
e membro do Grupo
Global Transparency
da WFA

Uma base de dados de sites comuns.

Uma base de dados de sites mantida por uma entidade independente, com métricas de qualidade e outros fatores chave de transparência, disponíveis de forma aberta e gratuita para ser acedida por todo o ecossistema. Se o investimento num site excede um determinado valor num determinado período, esse site deveria ser obrigado a registrar informações adicionais sobre os seus negócios de base de dados comum.

Uma base de dados comum de fornecedores tecnológicos de publicidade.

Com exceção das plataformas de anúncios mais conhecidas, pode ser difícil saber que empresa está por detrás de um determinado marcador *(tag)* de anúncio. Os marcadores com elevados volumes de manipulação estão frequentemente alojados em domínios com apenas semanas ou meses de idade, e utilizam um nome de domínio obscuro combinado com uma total proteção de privacidade. Mesmo que um investigador, com base nisto, queira criar uma imagem do fluxo de tráfego de anúncios e do fluxo de dinheiro, só seria possível a um nível relativamente superficial. Para combater eficazmente isto, é necessário uma base de dados comum de fornecedores. Este é um exemplo onde iniciativas do tipo Trustworthy Accountability Group (TAG*) nos EUA, desempenham um papel.

**TAG é um programa de responsabilidade entre indústrias. Um programa conjunto da indústria do marketing e da media, o TAG foi criado com foco em quatro áreas principais: tráfego de publicidade digital fraudulenta, combate à pirataria, pirataria na internet apoiada por anúncios e promoção da segurança da marca. O TAG foi criado pela Association of National Advertisers (ANA), pela American Association of Advertising Agencies (4A's), e pela Interactive Advertising Bureau (IAB) e trabalha com empresas em toda a cadeia digital de fornecimento de publicidade.* http://www.tagtoday.net/

4. GOVERNANÇA

Alterações contratuais.

Os contratos com agências e fornecedores parceiros devem ser revistos na medida em que a responsabilidade contratual se torne no fator-chave para a mudança de comportamento do parceiro. O foco deve estar nas penalizações por má colocação dos investimentos em inventário relacionado com fraude publicitária, quando a sua prevenção poderia ter sido razoavelmente conseguida.

Trabalhar com as autoridades.

Os anunciantes podem ajudar através da partilha de resultados e de dados, e relatando às autoridades competentes problemas significativos no ecossistema. A Associação Inglesa de Anunciantes (ISBA) lançou com a

**A ISBA trabalhou de perto com a Police Intellectual Property Crime Unit de Londres como parte de uma parceria única entre a policia e a industria digital do RU para combater a atividade ilegal relacionada com a publicidade online. O objetivo é proteger os anunciantes assegurando que os seus anúncios não aparecem em sites e IP's ilegais deixando-os morrer sem investimento de anunciantes.*

Pressionar para consequências legais iguais às de crimes semelhantes.

Porque não há precedente legal de sentenças, as entidades que aplicam as leis não estão dotadas dos recursos necessários para investigar seriamente crimes de fraude publicitária, independentemente do tamanho da operação ou outros fatores.

Solicitar reparações retroativas dos parceiros

As comissões/taxas cobradas pelo mercado de anúncios digitais em rede (e.g. Google AdWords, Yahoo Search Marketing), das plataformas de anúncios ou das agências onde as campanhas foram objeto de fraude publicitária devem ser devolvidas aos respetivos anunciantes. Solicitar essa reparação é importante porque vai indicar ao ecossistema de fornecedores que não é mais possível ganhar comissões por inação

"Este guia não é sobre atribuição de culpas. É sobre iniciar um caminho para encontrar soluções viáveis para os anunciantes. É necessária uma alteração de comportamentos de todos os atores deste ecossistema. Não apenas dos responsáveis das marcas mas de todos aqueles em quem confiamos o nosso orçamento, o que inclui as nossas agências."

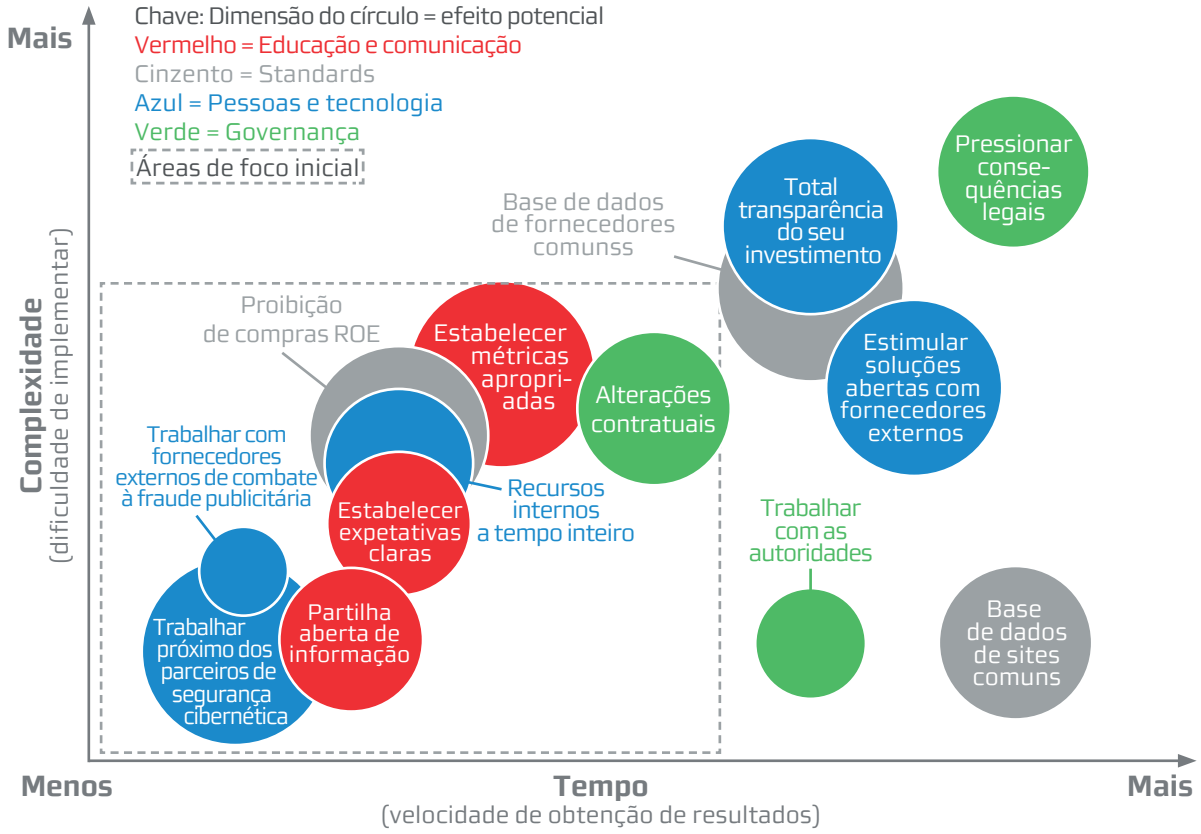
Sital Banerjee,
Global head of Media, Philips e membro do Global Transparency Group da WFA

O QUE PODEM OS ANUNCIANTES FAZER?

As ações descritas acima podem ser subdivididas por tempo (a rapidez com que produz resultados), efeito (a dimensão do resultado), e complexidade (a dificuldade de implementar).

Muitas das soluções abordadas neste documento caem no quadrante esquerdo do gráfico abaixo. Como são relativamente menos complexas e levam menos tempo a implementar são recomendas como 'áreas de foco inicial'. Trabalhar com parceiros de segurança cibernética e partilha de informação são claramente áreas a concentrar a atenção dada a relativa facilidade de implementação, enquanto a criação de métricas apropriadas pode ter o maior efeito global.

Do outro lado do espectro, não deve ser desconsiderada a pressão para consequências legais, face à relativa complexidade e tempo necessários para a implementação do processo. Não são muitos os sinais que podem ser dados ao mercado tão fortes quanto estes, e que veiculem a intenção da comunidade anunciante.



"O problema que enfrentamos é complexo e pode parecer intimidatório. Mas ignorá-lo, olhando para o lado, não é opção. Para muitas marcas que passaram as ultimas décadas ou mais, a defender grandes investimentos no digital, estas não são boas notícias.

A resposta não é abandonar o digital nem reprimir a inovação. Contudo precisamos de ter muito mais cautela e melhorar muito as nossas competências nesta luta. A WFA centrará os seus esforços em desenvolver ainda mais soluções para os seus membros, de forma a proteger as suas marcas e investimentos.

Compete ainda à totalidade da indústria aceitar a necessidade de mudança; pôr de lado interesses pessoais e abraçar o potencial de soluções abertas, semelhantes àquelas que têm provado ser eficazes noutros casos de cibercrime.

Isto não será fácil de resolver. Mas estamos coletivamente convencidos que a nossa indústria pode fazer face ao desafio, em benefício do ecossistema digital e da sociedade em geral ".

Stephan Loerke,
Chief Executieve Officer, WFA & membro do Global Transparency Group da WFA

GLOSSÁRIO

Empilhamento de anúncios (*Ad stacking*) > uma técnica de fraude em que múltiplos anúncios são servidos numa página única, eficazmente colocados uns em cima dos outros, o que significa que os colocados por baixo do que está no nível acima não são visíveis.

Extensão de audiência (*Audience extension*) > uma prática utilizada pelos *publishers* em situações em que não conseguem dar responder à procura do seu de inventário publicitário. O editor pode utilizar os dados da sua audiência própria (*first-party*) para comprar a mesma audiência noutros sites e vender esse inventário como se fosse dele. Esta técnica arrisca uma queda significativa na qualidade do inventário Vs a qualidade do seu próprio inventário, deixando os anunciantes com a convicção que os seus anúncios estão a ser servidos apenas no site desse editor.

Robots da Internet (*Botnet*) > um *'bot'* é um tipo de *software* nocivo utilizado para controlar um computador ou um telemóvel infectados. Um grupo ou uma rede de máquinas que tenham sido co-optadas e, desta forma, estão sob o controle do mesmo atacante é conhecido como um "*botnet*".

Fraude de cliques (*Click fraud*) > quando cliques fraudulentos são reportados como legítimos.

Fraude de conversão (*Conversion fraud*) > quando as ações fraudulentas do utilizador, tais como inscrições para receber mais informações sobre um produto, são relatados como legítimas.

Empalhamento de *cookies* (*Cookie stuffing*) > uma técnica em que um *cookie* afiliado, é colocado no dispositivo de um utilizador a partir de um site terceiro, sem que este visite o site terceiro em questão.

Fraude de dados (*Data fraud*) > quando os dados (*first ou third-party*), são envenenados de maneira a que os *cookies* ou outros identificadores se ligam aos *bots* e não aos utilizadores. Noutros casos os identificadores podem estar associados corretamente aos utilizadores mas, em resultado de atividades fraudulentas, as ações podem ser reportadas de forma deturpada.

Dados próprios (*First party data*) > Os SEUS dados. Estes são dados recolhidos dos seus clientes/audiências e podem incluir: comportamentos, ações ou interesses demonstrados através do seu site(s); dados pessoais da sua base de dados de CRM; dados de subscrição; dados de redes sociais.

Fraude de exploração (*Fraud farms*) > uma abordagem humana, onde a fraude (tipicamente fraude de conversão), é executada a baixo custo por mão de obra barata, mais frequentemente encontrada em países em vias de desenvolvimento.

Fraude de impressões (*Impression fraud*) > quando impressões fraudulentas são reportadas como legítimas.
Sistema de Deteção de Intrusos (Intrusion *Detection Systems* (IDS)) > dispositivo ou software que controla as atividades da rede ou atividades do sistema para ações ilegais ou violação de políticas.

***Run Of Exchange/s* (*ROE*)** > uma opção de segmentação comumente utilizada, onde o inventário é comprado a partir de qualquer site de transações de anúncios, acessível através de uma determinada plataforma de compra de anúncios.

***Spamers* Sociais (*Social Spambots*)** > *bots* que partilham *links* das plataformas de redes sociais.

Tráfego comprado (Sourced Traffic) > tráfego falso que é comprado a partir do mercado de tráfego de origem. Normalmente, o tráfego é gerado a partir de barras de ferramentas (injeções) ou outro é qualquer *software* que processa automaticamente anúncios, a fim de gerar receitas para o seu autor (*adware*), cloudbots ou botnets convencionais, ou outras fontes fraudulentas.

Spam-sites > sites tipicamente focados em tráfego proveniente da arbitragem (compra num mercado de publicidade e venda noutro beneficiando da diferença temporária) legítima do ecossistema de publicidade online, ou que estão envolvidos noutras formas de atividade fraudulenta.

Dados de terceiros (*Third party* data) > são dados gerados noutras plataformas e frequentemente agregados a partir de outros sites. Podem ser usados para efeitos de *marketing* autónomo ou para aumentar e melhorar os dados próprios.

Rastreador da internet (*Web crawler*) > um *bot* da Internet que navega sistematicamente na *World Wide Web*, tipicamente para fins de classificação da Web.

Raspador da internet (*Web scraper*) > técnica de programação de computador para extração de informações de sites.

Botlab.io é uma fundação de investigação focada na pesquisa da fraude publicitária, violações de direitos do utilizador e outras práticas maliciosas, na cadeia de fornecimento tecnológico de publicidade. É o único grupo de defesa pública focado apenas no utilizador de internet e foi formada com pessoas de dentro, ex-profissionais da indústria da tecnologia publicitária e liderada por investigadores. Mikko Kotila é Responsável na Botlab.io, um veterano da publicidade na internet e um influenciador e inovador respeitado na indústria da publicidade tecnológica. Desde 2005 que Mikko investiga ativamente a fraude publicitária e tópicos relacionados, tem mais de 20 anos de experiência como investigador na internet e trabalha com a Botlab.io a tempo integral como voluntário. Mikko é co-autor destas orientações juntamente com a WFA.

Advertising Fraud Council é uma iniciativa colaborativa de investigação com curadoria de Botlab.io centrada na investigação avançada sobre o tema da fraude publicitária. O conselho desta organização é composto pelo líder da maior empresa de tecnologia publicitária contra a fraude, pelo CEO de uma *start-up* contra a fraude publicitária, por um investigador independente de segurança, por Ruben Cuevas Rumin, professor assistente na Universidade UC3M, por um consultor independente de fraude publicitária, Shailin Dhar, e por um líder sem remuneração. Os membros do conselho trabalham em conjunto, partilhando recursos e dados, juntando investigação e desenvolvimento.

WFA é a voz dos anunciantes em todo o mundo, representando 90% do investimento global de marketing - cerca de US $700 mil milhões por ano – através de uma rede global única constituída pelos maiores anunciantes do mundo. A WFA lidera a comunicação de marketing eficaz e responsável em todo o mundo.

apan associação portuguesa de anunciantes

Av, da República, 62F-6º andar
1050-197 Lisboa
✆ +351 21 796 96 92
✉ apan@apan,pt 🌐 www.apan.pt