

list en bedrog in digital - en wat ertegen te doen de click

OVER DE PRECIEZE OMVANG VAN ADVERTENTIE-FRAUDE HEERST VEEL ONDUIDELIJKHEID. Maar dat weerhoudt onderzoekers er niet van om met duizelingwekkende getallen te strooien. Zo meldde Bloomberg al in 2015 dat adfraude adverteerders 6,3 miljard dollar kostte. In een studie van de Amerikaanse Association of National Advertisers (ANA) en beveiligingsbedrijf White Ops, ruim twee jaar geleden, werd zelfs een bedrag van 7,2 miljard dollar genoemd. Russische criminelen zouden volgens ANA dagelijks tot 5 miljoen dollar aan de fraude verdienen.

Vorige maand verscheen het rapport *'State of the digital ad fraude'* van onafhankelijk onderzoeker Augustine Fou, die ook weer spreekt van een miljardenschade. Frou zegt dat de advertentiezwandel 'uit de hand loopt' door het inzetten van nepsites. En onlangs nog rapporteerde het Berlijnse bureau Adjust op basis van eigen fraudedetec-tiesoftware dat van alle betaalde appinstallaties in de

eerste drie maanden van 2018 liefst 7,3 procent frauduleus was. Forrester waarschuwt dan ook dat de schade in de VS nog verder zal oplopen, naar 10,9 miljard dollar in 2021.

Dat er zoveel verschillende cijfers de ronde doen, is deels te wijten aan de lastige afbakening van het fenomeen. Maar één ding is wel duidelijk: adfraude is onlosmakelijk verbonden met programmatische inkoop van digitale advertenties. Dit is een van de snelst groeiende segmenten van digitale marketing; bijna vier van elke vijf digitale advertentie-euro's worden programmatisch uitgegeven.

Niet alleen de inkoop wordt geautomatiseerd, soms geldt dat ook voor de consumptie. Zo doen clickbots het



Advertentiefraude kost het bedrijfsleven miljarden. Dat is althans het beeld dat wordt geschetst in internationale rapporten. Maar hoe dramatisch is de situatie echt? En wat kun je ertegen doen? *Een onderzoek naar de aard, schade en aanpak van een hardnekkige digitale plaag.*

fraude



'internet maakt gebruik van boterzachte metrics'

voorkomen alsof een advertentie door mensenogen is gezien, terwijl dat niet zo is. Ondertussen betaalt de adverteerder wel voor de views. Fraude dus.

alarmbellen

Klikfraude (botverkeer) is het bekendste en actiefste lid van de adfraude-familie. Het gaat hier om het onrechtmatig klikken op pay-per-click-advertenties om meer inkomsten te behalen. Dat klikken kan door mensenhanden worden gedaan (op zogenaamde 'clickfarms'), maar meestal wordt hiervoor software gebruikt (ook wel clickbots genoemd omdat er als het ware door 'robots' wordt geklikt). In dat geval schakelen de fraudeurs vaak complete computernetwerken in die ze op afstand besturen via door henzelf verspreide malware of virussen.

Klikfraude kan worden gespot wanneer er bijvoorbeeld veel kliks binnenkomen via één IP-adres, of wanneer er opvallend vaak wordt doorgeklikt. Alarmbellen kunnen ook gaan rinkelen als de conversie binnen het verkeer vanaf een bepaalde uitgever wel heel erg laag is.

neppende influencers

Een recentere frauduleuze trend is die van influencers die hun volgers 'kopen'. Daarmee pretenderen ze een groter bereik te hebben zodat zij hun tarief kunnen verhogen. Volgens Unilever-cmo Keith Weed heeft naar schatting 40 procent van de influencers al dan niet bewust nepvolgers. Dit gedrag ondermijnt het vertrouwen van de consument en vormt daarmee een regelrechte bedreiging voor deze jonge tak van reclame.

Unilever kondigde eerder deze maand al

aan om de banden met fake-accounts en fake-influencers te verbreken. Maddie Raedts, founder en cco van Influencer Marketing Agency IMA: 'Het is een lastige kwestie, maar niet een dusdanig groot probleem dat de volledige industrie erdoor kan instorten. Met de juiste kennis kun je frauderende influencers aanpakken.' Ook directeur Sonja Loth van Social.Inc. denkt dat je in influencer 'nep' prima kunt herkennen. 'Wanneer je op je hoede moet zijn? Als de resultaten te goed zijn om waar te zijn.'

Niet alleen influencers rommelen met hun bereikcijfers. Ook sociale platforms kunnen er wat van. Zo berichtte Nielsen onlangs dat de bereikcijfers van Facebookvideo's 94 procent lager liggen dan Facebook zelf beweert.

En zo zijn er nog wel meer vormen van 'gerommel' die misschien niet als regelrechte fraude kunnen worden betiteld, maar er toch wel tegenaan schurken.

crimineel gedrag

Bij IAB Nederland noemt directeur Yvonne de Jager adfraude een containerbegrip. 'De definitie is vaag.' De transparantiediscussie bijvoorbeeld rekent zij niet onder adfraude, viewability ook niet. Wat dan wel adfraude mag heten, daarover is De Jager helder: 'Dan hebben we het over non-human traffic. Dat is crimineel gedrag en moet worden bestraft.'

Marcel Vogels, oprichter van Memo2 en het DMA Institute, beaamt dat er veel misvattingen bestaan over adfraude. Vaak wordt er dan gewezen op het hoge percentage botverkeer, waarvan de Amerikaanse botbestrijder Distil Networks beweert dat het intensiever is dan het verkeer tussen mensen. Toch hoeft dat volgens Vogels absoluut geen indicatie van fraude te zijn. 'Er kruipen gewoon heel veel bot-trackers rond op het web. En het merendeel doet prima werk. Het gaat dan om geautomatiseerde systemen van zoekmachines en sociale mediasites die bijvoorbeeld websites indexeren, of die controleren of alle links op een website up-to-date zijn.'

nuchtere Nederlanders

De nuchtere toon van Marcel Vogels is kenmerkend voor de houding van Nederlandse marketeers. Bij de BVA bijvoorbeeld krijgen ze zelden vragen over adfraude, vertelt communicatiemanager Marion Moerman.

Ook Yvonne de Jager van IAB Nederland vindt dat het in ons land zo'n vaart niet loopt. 'Ons taalgebied is nu eenmaal zo klein dat het minder interessant is voor grootschalige aanvallen. In die zin zijn we best wel gezegend.' Ze wil daarmee het probleem allerminst bagatelliseren, en al helemaal niet ontkennen. 'Het bestaat natuurlijk wel. Adfraude houdt de groei van de sector tegen want het kan het vertrouwen ondermijnen, net als in bijvoorbeeld de financiële sector.'

Maar hoe zit het dan met XS4All, dat besloot om minder met programmatic te gaan doen? Dat heeft niks

VOORNAAMSTE VORMEN VAN ADFRAUDE

- klikfraude (botverkeer) nepkliks op pay-per-click-advertenties

- nepdomeinen doen alsof ze grote internetpublicaties zijn zodat adverteerders er ruimte inkopen die vervolgens bezocht wordt door bots

- fake-influencers influencers die met nepvolgers hun bereik (en vergoeding) verhogen

- affiliatefraude klikfraude die binnen een affiliatenetwerk wordt gepleegd

- snelle jongens dubieuze tussenpersonen en bureaus die verdienen aan onwetende uitgevers en adverteerders zonder een wezenlijke bijdrage te leveren.



VERGOEDINGEN

Google vergoedt marketeers automatisch wanneer hun advertenties worden bezocht door bots in plaats van mensen. Daarnaast zet het onder meer 180 filters en algoritmes in om deze vorm van fraude te bestrijden, stelde directeur productmanagement Payam Shodjai in een blogpost. Een aantal nieuwe features moet het makkelijker maken om te zien of en hoeveel invalide verkeer wordt gedetecteerd in advertentiecampaagnes en op welk moment dat gebeurt. Partijen als AppNexus, OpenX, Index Exchange, Teads, Telaria en DoubleClick Ad Exchange hebben toegezegd mee te doen aan het geautomatiseerde systeem. Bij een grote hoeveelheid invalide verkeer kunnen adverteerders tot dertig dagen na hun maandelijkse betaling een vergoeding aanvragen.

te maken met adfraude, zegt manager digital media Erik van der Kooij, maar komt voort uit de wens om 'goed te kunnen meten hoe zichtbaar onze advertenties zijn'.

zwarte doos

Gebrek aan transparantie geeft voeding aan twijfels over de effectiviteit van de bestedingen aan digitale reclame. Het zijn vooral de *big spenders* die zich hierover uitspreken. Zo gaf Procter & Gamble vorig jaar 100 miljoen dollar minder uit aan online advertising, maar dat had geen effect op de omzet. Bij de vraag naar effectiviteit speelt een ander probleem dan adfraude, zegt Marcel Vogels. 'Internet maakt gebruik van allerlei metrics die ogenschijnlijk zekerheid bieden, maar boterzacht zijn.' Hij geeft drie voorbeelden:

1. Impressies

'Een impressie wil niets anders zeggen dan dat een website een oproep doet aan een aderving-systeem voor het inladen van een banner. Het zegt helemaal niets over of die ad is geladen.'

2. Kliks

'Kunnen van een mens zijn, maar net zo goed van een bot.'

3. Uniek bereik

'Wat zegt dat? Met een veelheid aan digitale devices, kan een individu wel tien keer als unieke bezoeker worden geteld.' Wanneer marketeers dergelijke vragen aan hun mediabureau voorleggen, klinkt er volgens Vogels vaak een oorverdovende stilte. 'Zo blijft onder het tafelkleed wat nu eigenlijk de waarde is van al die ingekochte media.'

Vage metrics lijken dus een reëler probleem dan adfraude. Verschillende experts menen dat adfraude een aantal jaren geleden een serieus probleem was, toen programmatic net van de grond kwam. Inmiddels zou het ecosysteem van de ergste uitwassen gezuiverd zijn door verbeterde technologie. Vogels: 'Impressies op fake-websites ten koste van de adverteerder, het zal ongetwijfeld bestaan. Maar het is van ondergeschikt belang.' Marketeers maken zich volgens hem meer zorgen over de vraag 'kom ik met mijn merk terecht waar ik terecht wil komen, en is de uiting die ik daar vertoon effectief?'

niet fris

Ook programmatic advertising-expert Maarten Roelofs meent dat het echte probleem van het programmatic inkoopproces niet schuilt in fake-sites, click-bots en dubieuze app-installs. Grotere boosdoener noemt hij de vele schakels die in dit proces zijn ingebouwd. Die zorgen ervoor dat een aanzienlijk percentage van de bannerprijs verdwijnt in zakken van partijen die weinig waarde toevoegen.

Die schakels zitten zowel aan de kant van uitgevers (verkoopkantoren die uitgevers beloven om hun inventory tegen optimale prijzen te verkopen) als aan de kant van adverteerders (mediabureaus die opdrachten binnen de organisatie doorschuiven en daarbij telkens een bedrag in rekening brengen). Het is allemaal niet fris. Maar fraude? Roelofs spreekt liever van een '*opportunity* waar partijen gebruik van maken'.

Als we met hem bellen is hij juist op weg naar een klant: een uitgever die vermoedt dat jarenlang 80 procent van elke advertentie-euro is afgeroomd. 'Handmatige inkoop via een bureau kan zelden op tegen de algoritmes van Google en Facebook. Onlangs publiceerde een van de grootste marktpartijen zelf de uitslag van een interne competitie: artificial intelligence nam het op tegen een senior planner. Wat denk je? De planner verloor.' Steeds meer adverteerders halen de technologie nu zelf in huis en huren experts in voor analyse, constateert Roelofs. 'Daardoor zijn er minder gevallen waarin marge verdwijnt, maar de schade wordt juist groter. Om hun marges op peil te houden moeten bureaus met veel onderliggende schakels nu meer rendement maken op klanten die denken wel hulp nodig te hebben.'

blijven vechten

Om adfraude tegen te gaan, introduceerde IAB Europe oktober vorig jaar ads.txt. Dit initiatief laat bedrijven die advertentieruimte hebben, aangeven wie de ruimte mag verkopen. De tool garandeert dat degene die ruimte aanbiedt op een druk bezochte pagina ook echt de eigenaar is. Ads.txt - voluit: Authorized Digital Sellers - moet zo transparantie bij programmatic inkoop bevorderen en fraude voorkomen. 'In Nederland is dat door de hele keten ingevoerd', weet IAB-directeur Yvonne de Jager. 'Daarmee is een deel van de problemen ook gelijk opgelost.'

Ook Google is zeer actief in het bestrijden van adfraude. In het hoofkantoor in Dublin vertelt een woordvoerder dat Google advertentiefraude als een complexe uitdaging ziet, 'waar wij tegen blijven vechten'. Zo komt er met behulp van ads.txt nieuwe bescherming op de Google-platformen tegen domein-spoofing. 'Ook introduceerden we geautomatiseerde, proactieve refunds voor adverteerders, evenals nieuwe rapportage-features, zodat zij kunnen zien waar ongeldig verkeer binnenkomt.'



NEPACCOUNTS

Facebook heeft in het eerste kwartaal van 2018 wereldwijd 583 miljoen nepaccounts verwijderd. In diezelfde periode heeft het sociale netwerk ook 837 miljoen spam- en 2,5 miljoen haatberichten verwijderd. Dat maakt Nathaniel Gleicher, hoofd digitaleveiligheidsbeleid van Facebook, onlangs bekend. Veel van de accounts en spam- en haatberichten zijn offline gehaald voordat ze door iemand gerapporteerd werden. Facebook maakt daarvoor gebruik van technologie die automatisch ongewenste berichten kan herkennen. Hoe groot het aandeel is dat automatisch verwijderd is, zegt Gleicher er niet bij.

Het merendeel van dat verkeer wordt volgens Google eruit gefilterd voordat het de adverteerders raakt. 'De afgelopen vijftien jaar hebben we daarvoor een uitgebreid systeem ontwikkeld - van eenvoudige filters tot grootschalige machine learning-systemen.'

Verder belooft de woordvoerder dat het bedrijf adverteerders niets rekent voor alle ongeldige verkeer dat wordt gemeld en door Google bevestigd. Bovenal drukt Google marketeers en merken op het hart om alleen geautoriseerd in te kopen via ads.txt.

handmatig zoeken

Toch is dit allemaal volgens sommigen niet genoeg. Er zijn talloze techbedrijven die adverteerders willen ondersteunen met 'broodnodige' softwareoplossingen. Zoals de Amsterdamse fraudebestrijder Nexus Solutions. Wat doet het bedrijf dat Google en ads.txt niet al doen? Allereerst handmatig en actief zoeken naar patronen van klikfraude, zegt Feisal Hensbergen. 'Google heeft al geruime tijd een algoritme tegen ongeldige en frauduleuze klikken, maar wij merken dat daar nog heel veel doorheen komt.'

Vervolgens detecteert en registreert Nexus met behulp van geavanceerde software de kliks die toch doorkomen en blokkeert diegene die het frauduleuze patroon vertonen. Tot slot verzoekt het bedrijf Google op regelmatige basis - met succes - om restitutie. 'Dit betekent dat

het budget van onze klanten beter besteed wordt en de campagnes beter bestand zijn tegen adfraude.'

blinde vlek

Niet alleen marktpartijen moeten hun verantwoordelijkheid nemen, dat geldt ook voor marketeers, vindt Ruben Schreurs. Hij is directeur van Digital Decisions, een consultancybureau dat adverteerders helpt om controle te krijgen over hun digitale marketing.

Schreurs die eerder bij verschillende programmatic trading desks werkte en de *tricks of the trade* van binnenuit kent, zegt dat marketeers allereerst inzage moeten vragen in de campagnerapportages. 'Vaak blijken rapportages van hun bureau erg beperkt. Zo krijgen ze nog steeds geen volledig overzicht van alle domeinen waarop de campagne is ingekocht of hoe effectief de plaatsingen zijn geweest, terwijl dit al jaren standaardrapportages binnen de gebruikte systemen zijn.'

Adverteerders weten ook niet altijd welke data beschikbaar zijn, wat het lastig maakt om de juiste vragen te stellen aan de mediapartners. En dat maakt ze kwetsbaar, juist als er een vermoeden is van fraude.

Schreurs adviseert adverteerders daarom de licenties van technologie voor programmatic-inkoop in eigen huis te halen, zodat ze zelf toegang hebben tot de data. 'Het bureau kan nog steeds de inkoop verzorgen, maar als adverteerder heb je volledig inzicht en totale controle over de inzet.'

Ook noemt hij *adverification*-oplossingen die in detail laten zien hoe effectief campagnes zijn ingekocht. 'Hiermee zie je niet alleen waar een uiting te zien is, maar ook aan wie die werd getoond, of de content waarbij de advertentie geplaatst werd 'brand safe' was, enzovoorts. De informatie die je uit dit soort systemen haalt is erg uitgebreid, wat helpt om de inkoop samen met je bureau efficiënter te maken.'

Een keihard bewijs van adfraude leveren de beschikbare *adverification*-tools niet volgens Schreurs. Ze kunnen bijvoorbeeld niet zien of een klik van een clickfarm of een bot komt. Daarbij komt dat ze verschillen in de manier waarop ze impressies en kliks analyseren, wat betekent dat verschillende tools andere resultaten rapporteren. Vandaar ook de sterk uiteenlopende schattingen over de omvang van adfraude.

Bovendien, weet Schreurs, hebben ze een blinde vlek voor nieuwe, innovatieve vormen van fraude, zoals influencers met fakevolgers. Marketeers staren zich vaak blind op aantallen volgers (bereik), maar zouden zich beter kunnen verdiepen in zaken als de ratio tussen engagement en volgers, demografische kenmerken van de doelgroep en groeipercentage, concludeert hij. ◀

TEKST ROB BEEMSTER EN ROBERT HEEG

'marketeers krijgen nog steeds geen volledige rapportages'

