



AD FRAUD



DELTA PROJECTS

HISTORIE

Det er over 20 år siden den første bannerannonseren ble publisert, og mye har skjedd siden den gang. Veksten i bruk av internett har vokst enormt verden over, hvorpå man nå teller over 3 milliarder aktive brukere hver dag. Like imponerende er fremveksten og utviklingen av annonseteknologi og digital annonsering.

Med lanseringen av prestasjonsbaserte programmer (affiliate), økte behovet for å måle blant annet klikk med tanke på kampanjenes KPI. Som et resultat økte antallet aktører som kunne levere klikk og trafikk til nettverk og affiliates (nettsider, portaler med mer). Et god eksempel var de såkalte klikk-programmene; personer fikk betalt for å bruke dagene til å klikke på bannerannonser. Med utviklingen av mer automatiserte løsninger flyttet aktørene seg over til denne formen. Ved siden av dette hadde man ad op teams som begeistret seg over å kunne kjøpe mengder av billig trafikk, hvorpå de tidvis så bort fra kvalitetsaspektet. På selgersiden har man sett at publisistene har kunnet sikre seg annonseinntekter ved å øke andelen falsk trafikk, som igjen annonsebørsene har fått sin del av. Dette har igjen forflyttet seg til annonsørene som har blitt presentert gode resultater og tall. Å møte kampanjenes KPI rundt visninger og klikk har vært enkel, men det reduserer også selve kvaliteten på annonsene.

Heldigvis, med fremveksten av programmatiske kjøp, har dette problemet blitt bragt frem og ut i lyset. I og med at premium-publisistene går programmatisk og der igjen de seriøse aktørene, ser man at det nå jobbes aktivt med å oppdage ad fraud (falsk trafikk).



ULKE TYPER AD FRAUD

LAUNDERED IMPRESSIONS

Laundered impressions, eller hvitvaskede annonsevisninger som man gjerne kaller det, betyr rett og slett at en trafikk-kilde utgir seg for å være en annen publisist. Et eksempel kan være de typiske fildelingsnettverkene hvor man kan laste ned ulovlige filmer, programvare m.m. De fleste annonsører har ingen interesse av å ha sine bannere på denne typen nettsteder. Som et resultat av dette, kan enkelte manipulere hvordan det hele blir presentert i en annonsebørs, hvilket leder annonsøren til å tro at man kjøper annonseplass på gode nettsider. Så hvordan kan dette påvirke annonsørens markedsføring? Først og fremst ledes man til å tro at man kjøper plasseringer på et legitimt sted, mens annonsene i virkeligheten vises et annet sted. Disse plasseringene kan også være i strid med interne rettingslinjer men gjerne også fra ulovlige nettsteder.

AD STABLING

Ad stabling er når flere annonser blir eksponert i samme inntrykk. Annonsene kan enten bli lagt på toppen av hverandre, hvor bare den øverste vil være synlig for den besøkende, eller plasseres umiddelbart ved siden av hverandre. I sistnevnte tilfelle blir annonsene vist i en klynge, og vil være vanskelig å skille fra hverandre. Dette betyr igjen at annonsører betaler for annonser som ikke er synlige eller knapt synlig og vist i et heller dårlig annonsemiljø.

COOKIE STUFFING

Dersom en bruker mottar flere cookies fra flere annonsører enn faktiske klikk, snakker man gjerne om Cookie stuffing. Denne typen svindel tar sikte på å sikre seg provisjoner. Et eksempel kan være dersom en blogger sender en besøkende til en nettbutikk hvor et kjøp blir gjort. Bloggeren vil dermed kunne få en liten prosentandel av salget. Med cookie stuffing kan en annen publisist regelrett ta æren for dette salget ved å droppe flere cookies i brukerens nettleser. Jo flere cookies som droppes, jo større blir gjerne sjansen for at personen vil besøke en av nettbutikkene. Dette betyr at markedsføreren betaler ut provisjon for salg som ikke kan relateres til kampanjen, samt at det også har en negativ innvirkningen på nøyaktigheten, rapporteringen og det faktiske resultatet.





PIXEL STUFFING

Pixel stuffing er når en 1x1 piksel er plassert på et nettsted, som igjen laster opp et helt annet nettsted. Det vil være umulig for brukeren å se den "nye" nettsiden, men det vil bli registrert seg som en visning. Denne praksisen er ofte kombinert sammen med cookie stuffing hvor den skjulte nettsiden inneholder cookies. Dette resulterer i at annonsører betaler for annonser som ikke er synlig for brukeren.

FALSKE NETTSTEDER

Falske nettsteder er nettsteder uten menneskelig trafikk. De er bygget utelukkende for reklame og tilbyr ikke noe innhold. Disse områdene er ofte en del av større nettverk. Dette for å unngå at hver enkelt nettside ikke generer for store inntekter så man måtte fatte mistanke. Det er imidlertid kjent at aktørene bak slike falske nettverk kan generere betydelig omsetning. For en annonsør betyr dette at man kjøper verdiløse visninger siden ingen mennesker faktisk ser annonsene.

VERKTØYLINJE

Verktøylinjen, oftest kalt tool bars, går ut på at egne annonser blir lagt ovenpå andres annonseplasser. Det kan igjen lede annonsøren til å tro at man kjøper bedre plassering enn hva som faktisk er tilfellet.

FALSKE KLIKK

Klikksvindel er når en person, bot eller et automatisert skript klikker på en annonse bare for å generere et klikk. Disse klikkene vil bli registrert og presentert i kampanjerapportene, men er regelrett sløsing med budsjettet. Dette siden "klikkeren" aldri vil ha til hensikt å gjøre et kjøp. Videre kan disse klikkene aktivere CTR-optimalisering som igjen øker budene på disse annonseplasseringene. Med trafikken ledet til denne typen nettsider, vil også kampanjens resultat og rapportering bli svekket, noe som resulterer i ødeleggelse av økosystemet.

IKKE-MENNESKELIGE TRAFIKK

Her snakker man om visninger og klikk som kommer fra bot applikasjoner. Disse dataprogrammene er sofistikerte nok til å kopiere menneskelig nettleaseratferd og utføre automatiserte oppgaver. Dette resulterer i og påvirker markedsføreren til å kjøpe verdiløse visninger og klikk, dette da ingen mennesker har blitt eksponert for nettannonsen.

HVORDAN KAN MAN SÅ BESKYTTE SEG?

Annonsesvindel forekommer og kan følgelig bli kostbart, men det finnes måter å beskytte seg mot dette.

1. **Bare jobb med pålitelige partnere.**

Sørg for å velge en teknisk leverandør som tar dette på alvor og kan vise deg hvordan de håndterer dette. De bør ha klare rutiner for å oppdage og eliminere falske tall og resultater. Sørg for at de har såkalte White lists hvor man trygt kan la sine annonser kjøre, samt at alt annet fjernes.

2. **Sørg for at din tekniske leverandør har systemer for å oppdage svindel.**

Leverandøren skal ha både manuell og automatisk svindeldeteksjon for å sikre at all uredelig atferd blir identifisert og fjernet. De bør alltid sammenligne klikk og visninger for å sørge for at kommer fra samme land, samt at "bid" og "source" URL er de samme.

3. **Utvid dine ytelsesmål.**

Upålitelige markedsaktører kan lett tukle med beregninger som CTR eller CPM - det er lett å forfalske et klikk. Ved å fokusere mer på beregninger som CPO kan man effektivt unngå falske resultater.

Hvordan forebygge annonsesvindel, se link:

http://www.deltaprojects.com/assets/delta_adfraud_no.pdf

Delta Projects
Country Manager
Peter Karlsson



Om Delta Projects

Delta Projects tilbyr en unik og komplett plattform for planlegging, gjennomføring og rapportering av programmatisk kjøp. Vi er størst i Europa når det kommer til å ha sin egenutviklede teknologi, hvorpå mer enn 65 000 budforespørsler blir analysert hvert sekund. Det gir oss innsikten og verktøyet som trengs for å kjøre mest mulig effektive kampanjer. På tvers av vår plattform, sørger sanntidsdata for at budene du byr og kjøper samsvarer med den faktiske verdien av inventaret og målgruppen.

Delta Projects ble grunnlagt i Stockholm i 2002 , og har en lang historie med å bringe ny teknologi til markedet. Selskapet har en sterk tilstedeværelse i Nord-Europa med lokal tilstedeværelse i form av kontorer i både Sverige , Norge , Danmark, Tyskland og Nederland. Hos oss finner man alltid lokal medieekspertise og støtte. John Lilja er grunnlegger og CEO.

For mer informasjon vennligst besøk oss på www.deltaprojects.com.



DELTA PROJECTS