

مقابله با تقلب در صنعت تبلیغات موبایلی



فهرست مطالب

مقدمه	۳
وضعیت کنونی قلب در تبلیغات موبایلی	۵
منظور از قلب در تبلیغات موبایلی چیست؟	۵
قلب در تبلیغات موبایلی در یک نگاه	۷
انواع قلب در تبلیغات	۱۲
چه کسانی مدیریت مبارزه با قلب در تبلیغات را بر عهده دارند؟	۱۸
دستاوردهای تپسل در مبارزه با قلب در تبلیغات	۲۲
مصورسازی و نظارت بر داده‌ها	۲۳
الگوریتم تشخیص قلب اختصاصی تپسل	۲۴
روش مبارزه با قلب با کمک Third Party ها	۲۷
نتیجه‌گیری	۲۹



مقدمه

مانند اکثر نوآوری‌های تکنولوژیک و غیر تکنولوژیک در جوامع بشری اعم از دستگاه چاپ، رادیو، سینما، تلویزیون و اینترنت، پیدایش گوشی‌های هوشمند یا همان اسمارت فون‌ها زندگی همه ما را متحول کرده است. البته هیچ یک از تکنولوژی‌های گذشته و رسانه‌های جمعی به سرعت گوشی‌های هوشمند فراگیر نشدند. امروزه نزدیک به سه میلیارد نفر از مردم دنیا از گوشی‌های هوشمند استفاده می‌کنند.

نتایج تحقیقات بازار در شرکت zenith نشان می‌دهد هزینه جهانی صرف شده برای تبلیغات بر روی تلفن‌های همراه افزایش خواهد داشت و از **۱۵ درصد** در سال ۲۰۱۶ به ۲۶ درصد در سال ۲۰۱۹ می‌رسد. در حالی که روند تبلیغات بر روی سایت‌ها، تلویزیون، رادیو، روزنامه و مجلات رو به کاهش است.

اما هر چقدر بازار برای تبلیغات بر روی تلفن همراه رونق بیشتری پیدا کند، احتمال تقلب و یا سوء استفاده افراد نیز بیشتر می‌شود و تبلیغات تقلبی نیز رشد می‌کند و پیچیده‌تر می‌شود. در واقع عده‌ای دائماً در حال تلاش برای دستیابی و دستکاری هزینه‌های پرداختی برای تبلیغات هستند.

براساس تحقیقات انجام شده، ترافیک قلبی و کلیک‌هایی که به وسیله ربات‌ها انجام می‌شوند، **۷.۲ میلیارد دلار** هزینه اضافی در صنعت تبلیغات ایجاد می‌کند. بر این اساس فدراسیون جهانی تبلیغات پیش‌بینی می‌کند صنعت تبلیغات بعد از دارو، بیشترین آمار کلاهبرداری را خواهد داشت و تا سال ۲۰۲۵ رقم آن به **۵۰ میلیارد دلار** می‌رسد.

نکته قابل تأمل این است که عملکرد ضعیف تبلیغات و تبلیغات جعلی به برند و تصور عمومی درباره کل صنعت تبلیغات آسیب وارد می‌کند و وقتی این اعتماد تخریب شود به سختی بازسازی خواهد شد و هر روز شاهد رشد سریع تولید و استفاده از ابزارهای بلاک تبلیغات در موبایل و دسکتاپ خواهیم بود.

هدف این کتاب الکترونیکی بیان کلیات مربوط به تقلب در تبلیغات موبایل است و انواع مختلف تقلب در تبلیغات موبایلی و راهکارهای [شرکت تپسل](#) برای مقابله با آن‌ها بیان خواهد شد.

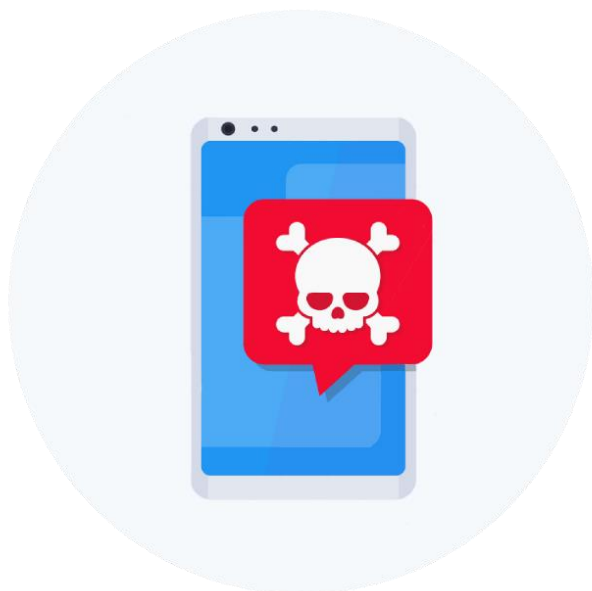
تیم تپسل به عنوان یک شبکه هوشمند تبلیغات به فرآیند تقلب در تبلیغات موبایل توجه ویژه داشته است و با انجام تحقیقات وسیعی در این زمینه راهکارهای جدی برای مقابله با آن ارائه کرده است.



۲۰۲۵



۲۰۱۶



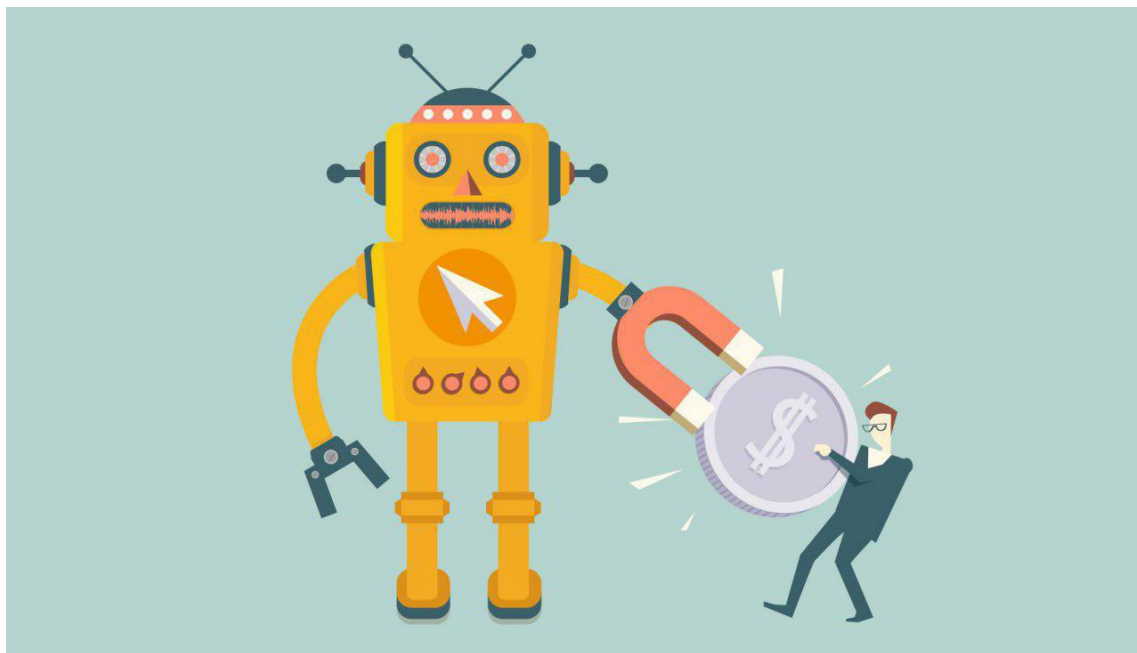
وضعیت کنونی قلب در تبلیغات موبایلی

منظور از قلب در تبلیغات موبایلی چیست؟

بعضی افراد و یا شبکه‌های تبلیغاتی غیر رسمی از روش‌های نادرستی برای کسب درآمد در تبلیغات موبایل استفاده می‌کنند. این افراد با استفاده از ربات‌ها و یا روش‌های خاص سعی می‌کنند impression سایت و یا اپلیکیشن‌های موبایلی را بالا نشان دهند. آن‌ها با تولید آمار بازدیدها، کلیک‌ها و نصب‌های غیرواقعی و تقلبی، عملکرد تبلیغات را بالا نشان می‌دهند و از این طریق از شبکه‌های تبلیغاتی قانونی و تبلیغ‌دهندگان، پول زیادی دریافت می‌کنند. چرا که تبلیغ‌دهندگان بر اساس تعداد این impressionها پول پرداخت می‌کنند و تصور می‌کنند این impressionها توسط کاربر واقعی اتفاق افتاده است. در حالی که برای impressionهای غیرواقعی پول پرداخت کرده‌اند.

علاوه بر بحث impressionهای غیرواقعی، شکل‌های دیگر قلب مانند دستکاری در نرخ کلیک‌ها، نرخ تبدیل (conversion rate) و یا موارد دیگر مانند فعالیت در اپلیکیشن‌ها و یا تعداد نصب که می‌تواند نشان‌دهنده عکس العمل یک کاربر واقعی نسبت به تبلیغات باشد را می‌توان نام برد. هم چنین در attribution نیز احتمال تقلب‌هایی وجود دارد. در واقع پلتفرم‌های تبلیغاتی نامعتبر تلاش می‌کنند، کاربرانی که در حال خرید هستند و یا تصمیم به خرید دارند را شناسایی کنند و هدف تبلیغات خود قرار دهند. سپس رفتار خرید آنان که ممکن است نتیجه تبلیغات یک شبکه معتبر دیگر باشد، به تبلیغات خود نسبت دهند و از این راه کسب درآمد کنند.

اغلب این تقلب‌ها که امروزه اتفاق می‌افتند با استفاده از ربات‌ها انجام می‌شوند. ربات‌ها برنامه‌های نرم‌افزاری هستند که برای انجام فعالیت‌های تکراری با سرعت بالا طراحی شده‌اند. افراد متقلب در سطح وسیعی از ربات‌ها برای فعالیت‌های غیر قانونی خود استفاده می‌کنند. آن‌ها به وسیله ربات‌ها، در ترافیک سایت و اپلیکیشن‌های با ظاهر درست و قانونی دست می‌برند و با دستکاری حتی به اپلیکیشن‌های دیگر وانمود می‌کنند که فعالیتی توسط یک کاربر در آن‌ها در حال انجام است. در این مرحله این افراد ممکن است افرادی را با حقوق پایین برای انجام کارهای ساده و تکراری مثل دانلود یک اپلیکیشن و یا صرفاً چند کلیک بر روی لینک‌های خاص استخدام کنند. هدف آن‌ها افزایش رتبه سایت و اپلیکیشن خود است که این هدف صرفاً نیاز به چند کلیک دارد



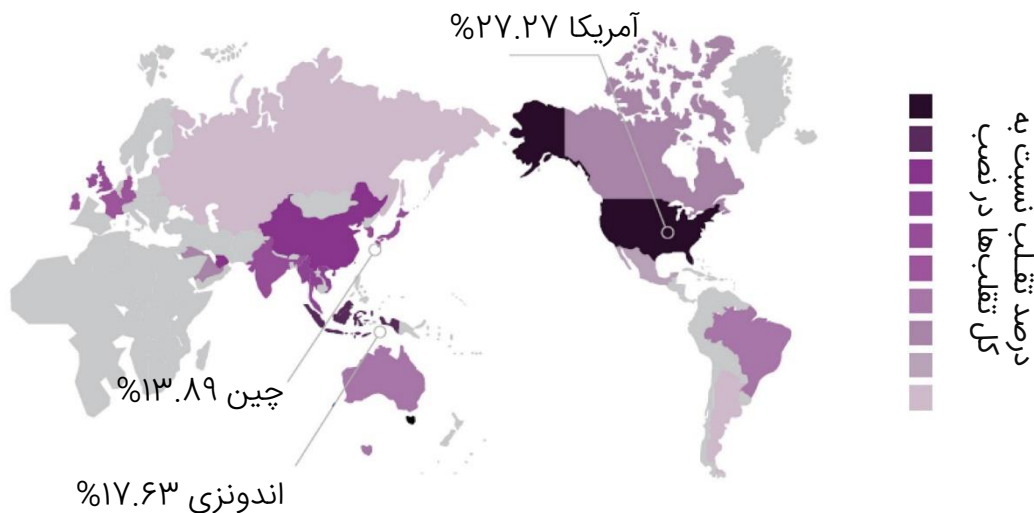
تقلب در تبلیغات موبایلی در یک نگاه

در شکل زیر میزان تقلب در تبلیغات موبایلی قابل مشاهده است. این داده‌ها بر اساس آنالیز ترافیک جهانی (همه ۱۹۶ کشور جهان) در تبلیغات در شبکه Mobvista در ماه‌های January و June در سال ۲۰۱۷ به دست آمده است.

توزیع محلی

داده‌ها نشان می‌دهد که سه کشور ایالات متحده، اندونزی و چین بیشترین آمار تقلب در حجم نصب اپلیکیشن‌ها از طریق تبلیغات موبایلی را داشته است که درصد آن به ترتیب برابر ۲۷.۲۷٪، ۱۷.۶۳٪ و ۱۳.۸۹٪ نسبت به کل تخلفات در حجم نصب است.

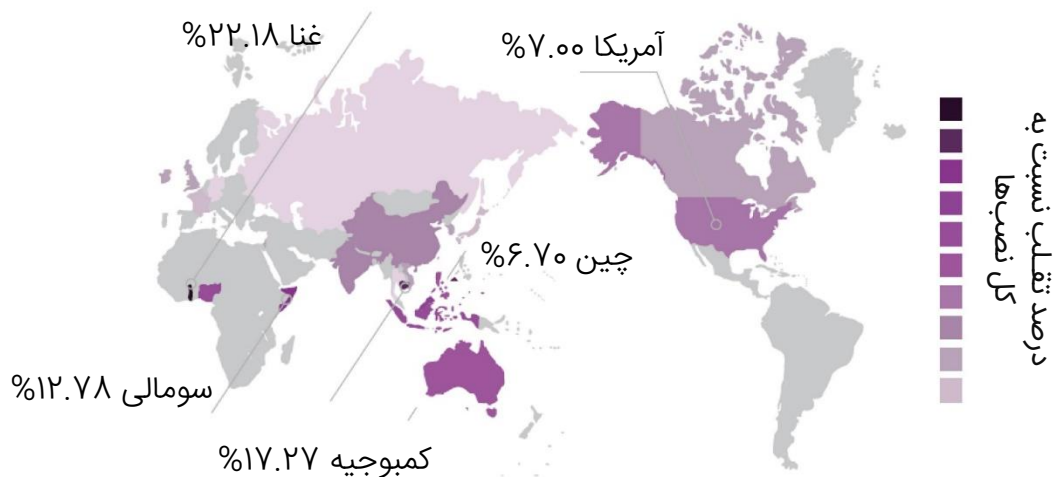
توزیع محلی تقلب در نصب (درصد محاسبه شده نسبت به حجم کل تخلفات جهانی در تبلیغات)





باید در نظر گرفت که این سه کشور بیشترین میزان ترافیک تبلیغاتی شبکه Mobvista را در جهان دارند. در نتیجه اگر درصد حجم تقلب نسبت به ترافیک را برای هر کشور محاسبه کنیم، این سه کشور همانطور که در تصویر نیز مشخص است، جزء کم تخلف ترین کشورها قرار می گیرند.

توزیع محلی تقلب در حجم نصب (درصد محاسبه شده نسبت به کل نصب صحیح و غیر صحیح (با تقلب) در آن منطقه)

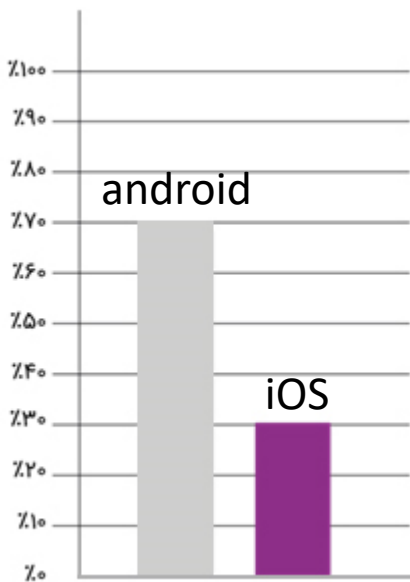


تقلب در حجم نصب؛ اندروید و iOS

داده‌های موجود نشان می‌دهد که در پلتفرم‌های موبایل، اندروید بسیار آسیب پذیرتر از iOS است. تحقیقات تیم Mobvista نشان می‌دهد، ۷۰ درصد تخلفات نصب مربوط به اندروید و ۳۰ درصد آن مربوط به iOS است.

البته با توجه به اینکه ۹۰ درصد گوشی‌ها در حال حاضر با سیستم عامل اندروید کار می‌کنند، این آمار عجیب نیست.

نکته دیگر اینکه اندروید پلتفرمی است که کاربران زیادی با دستگاه‌های قدیمی و یا نسخه‌های قدیمی این سیستم عامل در حال فعالیت هستند و همه کاربران، جدیدترین دستگاه‌ها و آخرین به‌روزرسانی را استفاده نمی‌کنند. در نتیجه نسبت به کدهای مخرب آسیب پذیرترند.



در حالی که google play store برنامه‌هایش را از نظر امنیت بررسی می‌کند. صدها app store دیگر وجود دارند که هوشیاری لازم را ندارند و افراد متخلف با استفاده از آن‌ها می‌توانند اپ‌های مخرب خود را وارد گوشی کاربران کنند.

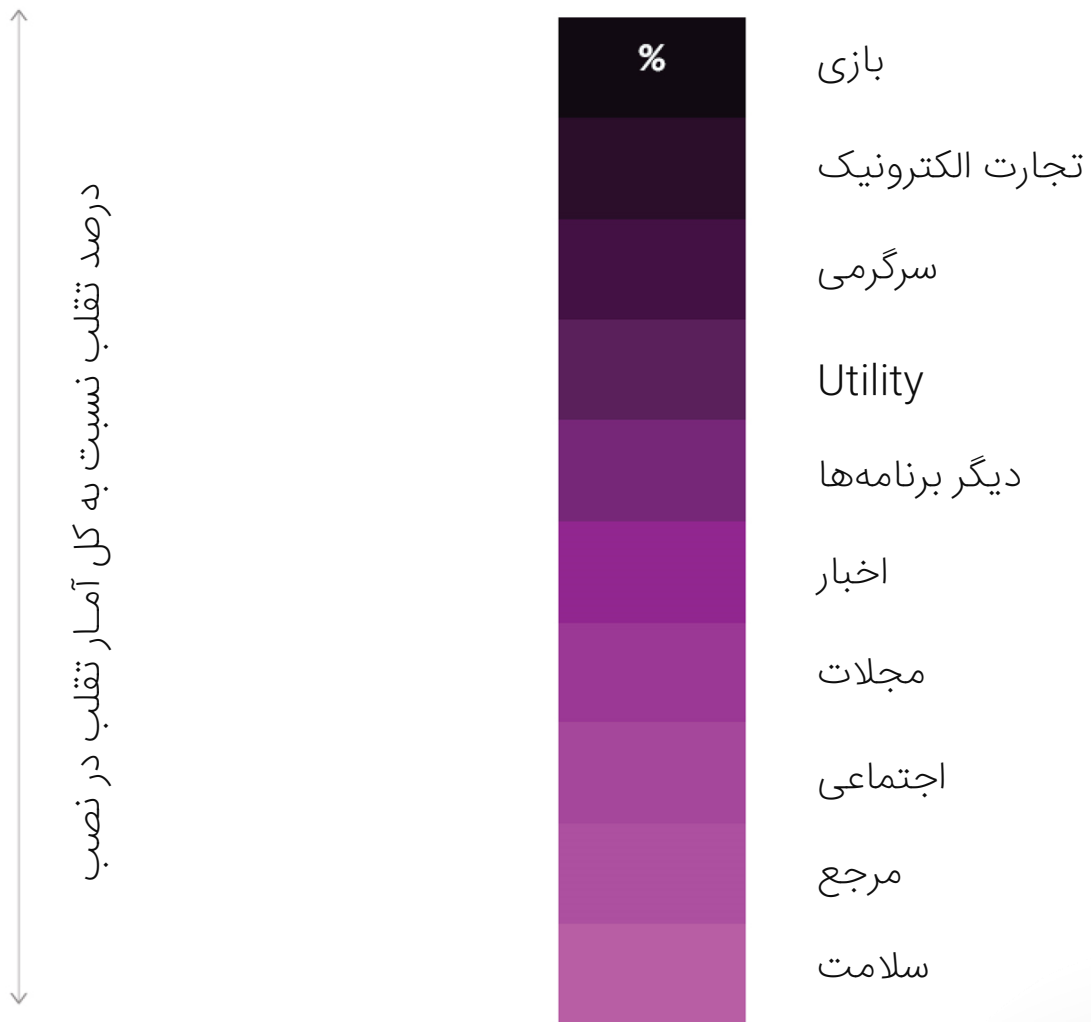
دلیل دیگر برای انتخاب اندروید توسط متخلفین برای فعالیت بیشتر، امکان تهیه اپلیکیشن‌هایی است که ظاهراً کاربری استاندارد و معمولی دارند ولی با کدهای پنهانی فعالیت‌های دیگری نیز روی تلفن شما انجام می‌دهند.



تقلب در انواع اپلیکیشن‌ها

به طور تقریبی حدود ده درصد از تقلب در نصب برنامه‌ها مشخص می‌شوند. همانطور که در تصویر می‌بینید اپلیکیشن‌های مورد هدف برای تقلب در نصب بیشتر از گروه بازی‌ها هستند. بعد از آن بیشترین تقلب در اپلیکیشن‌های تجارت الکترونیک (E-commerce)، سرگرمی و اپلیکیشن‌های utility است.

رتبه بندی گروه‌های مختلف اپلیکیشن‌ها بر اساس میزان تقلب



چرا اپلیکیشن‌های بازی نسبت به بقیه اپلیکیشن‌ها برای متقلبین جذاب‌ترند؟

دلیل آن این است که متقلبین از طریق این اپلیکیشن‌ها بهتر می‌توانند کسب درآمد کنند. بر اساس تحقیقات شرکت NewZoo، بازی‌ها ۴۶.۱ میلیارد دلار در سال ۲۰۱۷ ارزش مالی داشتند. هر روز بیش از ۵۰۰ بازی در اپ استورها اضافه می‌شود که هر کدام از آن‌ها می‌توانند هدف متقلبین قرار بگیرند. بر اساس اطلاعات شرکت appani، ۹۰ درصد درآمد گوگل‌پلی در سال ۲۰۱۶ از بازی‌ها به دست آمده است. در اپ استور اپل، ۷۵ درصد اپلیکیشن‌ها را بازی‌ها تشکیل می‌دهند. با این حال در کل، درآمدی که اپ استور اپل به دست می‌آورد بیشتر است. با توجه به آمار appani، اپ استور iOS، ۷ میلیارد درآمد بیشتری نسبت به گوگل‌پلی و بقیه اپ استورهای اندروید داشته است.

روش‌های رایگان و پولی بازاریابی برای
اپلیکیشن و راز و رمزهای کمپین‌های نصبی در
بلوک بازاریابی برای اپلیکیشن

[عضویت در بلوک](#)



انواع تقلب در تبلیغات

از منظر فرآیند، افراد متخلف از چهار نوع روش استفاده می‌کنند:

الف- تقلب در نمایش

ب- تقلب در کلیک

ت- تقلب در نصب و فعال سازی

ث- تقلب در داخل اپلیکیشن

همچنین از منظر کیفیت ترافیک فعالیت متخلفین را می‌توان به دو دسته تقسیم کرد:

ج- ترافیک تقلبی

ح- Attribution تقلبی

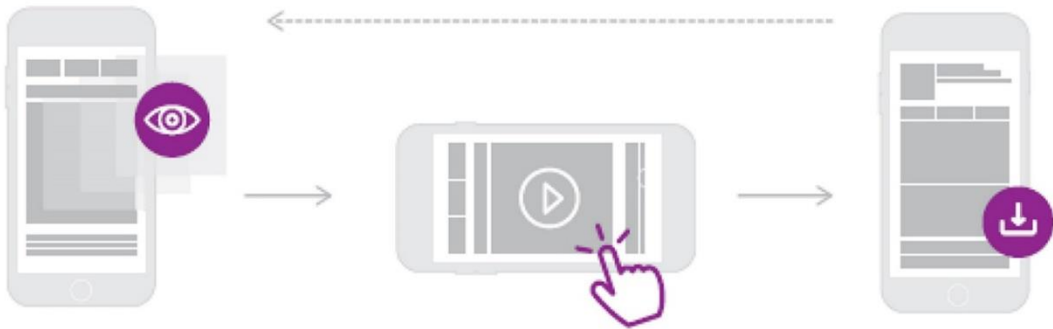
• تقلب در نمایش

• ترافیک تقلبی

• Attribution تقلبی

• تقلب در کلیک

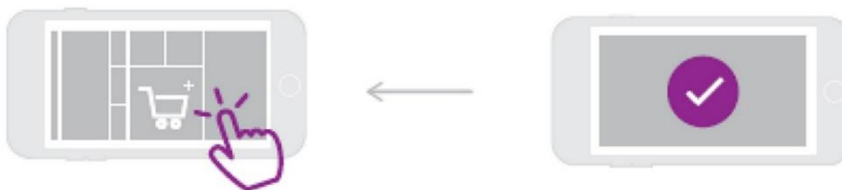
• تقلب در نصب و فعال سازی



اپلیکیشن را دانلود می‌کند. بر روی تبلیغ کلیک می‌کند. کاربر در حال دیدن تبلیغ است.

• تقلب در داخل اپلیکیشن

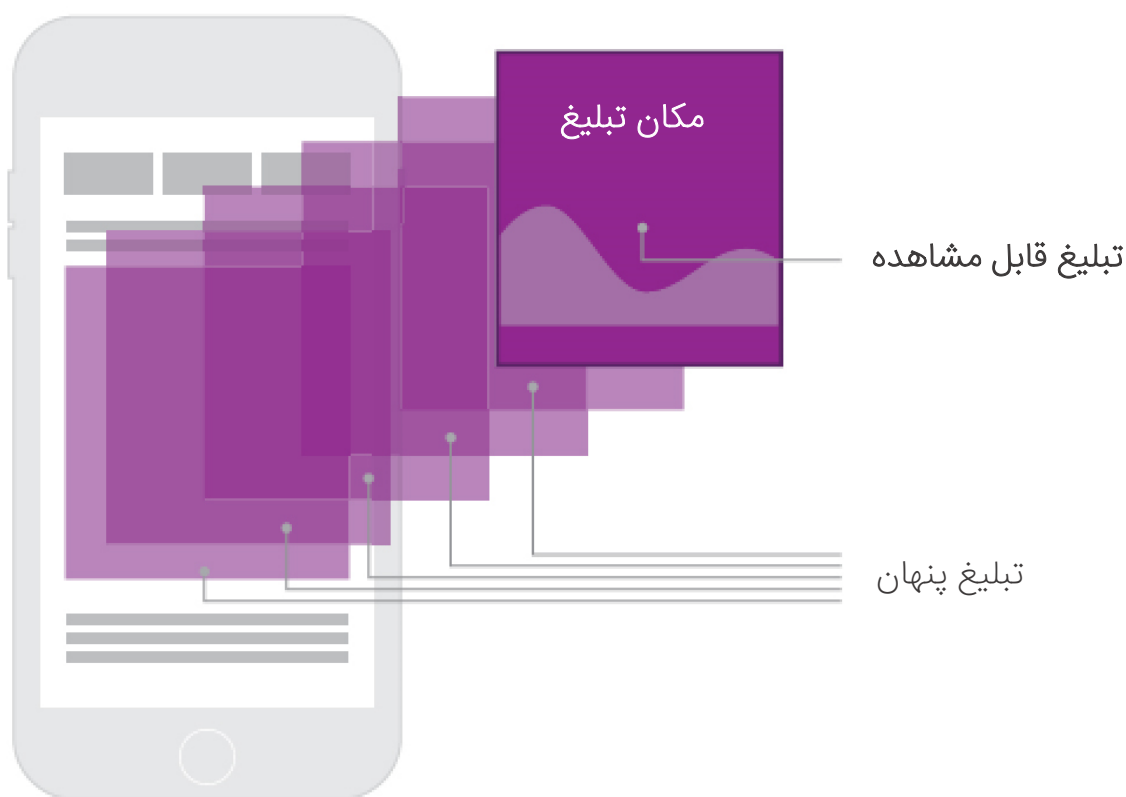
• تقلب در نصب و فعال سازی



اپلیکیشن برای اولین بار باز می‌شود. کاربر در داخل اپلیکیشن خرید می‌کند.

تقلب در نمایش

متداول‌ترین روش افراد متقلب این است که در مکانی که تبلیغات را قرار می‌دهند، چندین صفحه تبلیغ بر روی هم قرار دهند و کاربر تنها تبلیغی که بالای بقیه قرار گرفته را می‌بیند. در نتیجه در هر صفحه تبلیغ‌دهنده impressionهای متعددی بدون دیده شدن تبلیغ ثبت می‌کند و فقط یک تبلیغ از آن‌ها توسط کاربر قابل رویت است. به این روش ad stacking گفته می‌شود.



تقلب در کلیک

در این حالت فرد از ربات‌ها برای شبیه سازی رفتار کلیک کردن یک کاربر واقعی در حجم بالا استفاده می‌کند. اغلب به صورت پنهانی در اپلیکیشنی که ظاهراً استاندارد است و کارایی مناسبی دارد ربات‌هایی قرار داده می‌شوند که ترافیک برنامه‌ها را دستکاری می‌کنند و یا به نوعی با کلیک‌ها به برنامه القا می‌کند که فعالیت در آن‌ها در حال انجام است. به این کار click spoofing نیز گفته می‌شود.

تقلب کلیک می‌تواند با استخدام افرادی با هزینه‌های کم به جای کار با ربات‌ها انجام شود. هم چنین گاهی کاربران واقعی را تحریک به کلیک بر روی تبلیغات (اغلب غیر واقعی) می‌کنند. می‌توان هم click spoofing و هم ad stacking را در دسته تقلب کلیک قرار داد.



تقلب در نصب و فعال‌سازی

روش معمول متخلفین برای تقلب در نصب و فعال‌سازی استفاده از نرم‌افزارهایی است که نصب غیرواقعی ایجاد می‌کنند. گاهی نیز این کار را با ربات‌های کلیک انجام می‌دهند و در ادامه برای بالا بردن رتبه‌بندی آن اپلیکیشن در اپ استور افرادی را استخدام می‌کنند که کارهای ساده‌ای مثل دانلود اپلیکیشن و نصب آن را در دفعات بالا انجام دهند.

راهکار دیگر متقلبین استفاده از نرم‌افزارهای مخرب و تغییر اطلاعات دستگاه است و یا از کرک SDK اپلیکیشن برای فرستادن اطلاعات مجازی (مثل شبیه سازی دانلود یک اپلیکیشن) به اپ استور یا شبکه تبلیغاتی استفاده می‌کنند.

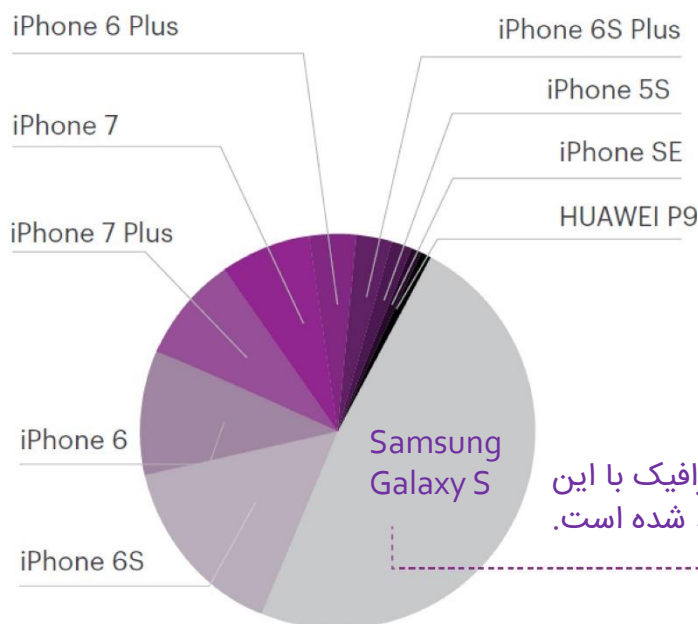


تقلب در داخل اپلیکیشن

نرخ استفاده و جذب کاربر برای اپلیکیشن‌ها مهم‌ترین شاخص برای بازاریابی در این حوزه است. به همین خاطر پرداخت به ازای فعالیت (cost per action یا CPA) از جمله پرداخت‌هایی است که ترجیح داده می‌شود که شرکت تپسل نیز این سرویس را به تبلیغ‌دهندگان ارائه می‌دهد. متقلبین این قسمت را نیز مورد هدف قرار داده‌اند. وقتی کاربران بر روی تبلیغات غیر واقعی آن‌ها کلیک می‌کنند، و به صفحه خرید وارد می‌شوند، همان نتایج متداول را خواهند دید، ولی آن کاربران که برای خرید، اکانت خود را شارژ نکرده‌اند و عملاً خریدی انجام نمی‌دهند، در شمارش به عنوان عملیات ناموفق به حساب نمی‌آیند. بنابراین، وقتی ناشر و یا تبلیغ‌دهنده داده‌های کمپین را بررسی می‌کنند، در بخش کسب درآمد آن مبلغ اغراق شده‌ای را می‌بینند. (با شمارش کلیک بر روی تبلیغات، هزینه‌های پرداخت نشده نیز در داده‌ها حساب شده است.) بنابراین، در پولی که برای شبکه تبلیغاتی در نظر گرفته می‌شود اغراق شده است.

ترافیک تقلبی

ترافیک تقلبی شامل همه موارد ترافیک مانند ترافیک ایجاد شده با ربات‌ها، ترافیک اضافه شده (incentivized traffic)، ترافیک ربوده شده از تلفن‌ها و ... می‌شود.



ناهنجاری در داده‌ها می‌تواند شامل حجم زیادی از ترافیک که به وسیله مدل‌های قدیمی گوشی‌ها تولید شده‌اند، باشد. این ترافیک با آنالیز توزیع (distribution analysis) قابل تشخیص است. برای تشخیص این نوع از تقلب، توزیع گوشی‌هایی که ترافیک را ایجاد کرده‌اند را با توزیع نرمال که با تلفن‌ها تولید می‌شود مقایسه می‌کنند.

بیش از نیمی از ترافیک با این مدل گوشی تولید شده است.

ترافیک تقلبی بر اساس رفتارهای کاربران نیز قابل تشخیص است. مثلاً اگر نرخ استفاده و بازگشت به اپلیکیشن (retention) در یک اپلیکیشن یک لحظه صفر شود و لحظه دیگر به ماکزیمم برسد و این تغییرات گاهی به سرعت و لحظه‌ای انجام شود، نشان دهنده این است که احتمالاً این ترافیک، تقلبی است.





Attribution تقلبی

در attribution تقلبی پلتفرم نامعتبر تلاش می‌کند کاربر نهایی که در حال انجام خرید است و یا معلوم است که قصد خرید دارد را تشخیص دهد و او را هدف تبلیغ قرار دهد. هدف نهایی این است که خرید آن فرد را به تبلیغات خود نسبت دهند، حتی اگر تحت تأثیر تبلیغات کمپین دیگری بوده است.

آشنایی با شاخص‌های
ابزارهای تحلیلی اپلیکیشن

[مشاهده مطلب](#)



چه کسانی مدیریت مبارزه با تقلب در تبلیغات را بر عهده دارند؟

با توجه به تعدد روش‌ها و حجم فعالیت‌های متخلفین در این حوزه گروه‌های مختلف در بازاریابی دیجیتال به فکر تشکیل گروه‌هایی برای مبارزه با تقلب در بازاریابی دیجیتال افتاده‌اند. فعالیت این گروه‌ها تحت عنوان آنتی فراد (anti fraud) شناخته می‌شود. این گروه‌ها با هدف جلوگیری از هدر رفتن بودجه‌های تبلیغاتی، حفظ جایگاه برند شبکه‌های تبلیغاتی و در نهایت حفاظت از اکوسیستم موبایل مارکتینگ که توسط متخلفین در حال تخریب است، شکل گرفته‌اند.

تبلیغ‌دهندگان

پلتفرم‌های ارزیابی در موبایل مارکتینگ

پلتفرم‌های تبلیغات

دیگر سرویس‌دهندگان در زمینه آنتی فراد

TUNE

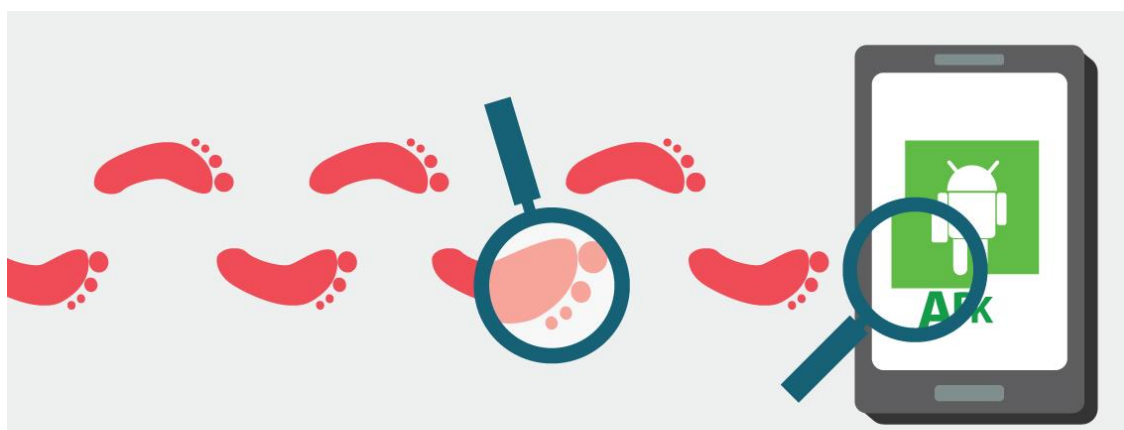
adjust

KOCHAVA★

AppsFlyer

TalkingData

پلتفرم‌های ارزیابی در موبایل مارکتینگ که در روبرو نام برده شده‌اند، از شناخته شده ترین سرویس دهندگان آنتی فراد در این حوزه هستند. Tune و Kochava در ایالات متحده، adjust در آلمان و talkingdata در چین فعالیت می‌کنند.



آشنایی با Trackerها
و روش انتخاب شمارنده مناسب

[مشاهده مطلب](#)

به طور کلی دو استراتژی در فعالیتهای آنتی فراد وجود دارد که توسط پلتفرمهای ارزیابی موبایل مارکتینگ (MMP) تدوین شده است:



فیلتر کردن IP

MMP برای شناسایی و رصد متخلفین یک بلک لیست تهیه می‌کند و این لیست را همیشه به روز نگه می‌دارد. اگر نصب IP غیرعادی باشد، آدرس‌های IP، شناسه سایت‌ها و شبکه‌هایی که متخلف شناخته می‌شوند در این لیست قرار می‌گیرند.

MMPها اگر IP نصب شده را غیر عادی ارزیابی کنند، attribution مربوط به آن را قبول نمی‌کنند. همچنین، نصب‌های مربوط به کاربران با ID ناشناس را نیز در داده‌های خود محاسبه نمی‌کنند.

اعتبار سنجی فعالیتهای

MMPها فعالیتهای مانند نصب و خرید را شناسایی و تأیید می‌کنند. این کار با بررسی رسیدهایی که در داده‌های سرور موجود است، انجام می‌شود.

برای نصب‌هایی که از سرور اپل استور و گوگل پلی دریافت می‌شود، MMPها یک رسید نصب دریافت می‌کند که قابل شناسایی است و سپس نصب‌هایی که قابل شناسایی نیستند را در شمار نصب‌های تقلبی قرار می‌دهند و تأیید نمی‌کنند.

در دریافت رسید از خریده‌ها در اندروید و iOS نیز MMP رسیدهایی که از سرورهای معتبر دریافت می‌کند را تأیید می‌کند و بقیه را در رده تقلب‌ها قرار می‌دهد.



همچنین مدل‌سازی‌های توزیع نیز از جمله استراتژی‌های محبوب است که MMP‌هایی مانند adjust، Kochava، AppsFlyer از آن‌ها استفاده می‌کنند. با استفاده از مدل‌های big data مثل MTTI (mean time to install)، CTTI (click to time install) و ... ناهنجاری‌های متداول را به خوبی تشخیص می‌دهند. MMP‌ها از مدل‌سازی‌های مختلفی استفاده می‌کنند که با یکدیگر تفاوت داشته باشند و تکنولوژی مورد استفاده آن‌ها هم‌پوشانی نداشته باشد.



اما نه تنها پلتفرم‌های attribution برای مبارزه با تقلب تلاش می‌کنند و فعالیت‌های آنتی فرد انجام می‌دهند، بلکه این وظیفه به عهده شبکه‌ها و پلتفرم‌های تبلیغاتی نیز می‌باشد که از این تخلف‌ها جلوگیری کنند.

چالش اصلی این است که افراد بسیاری هستند که با این روش‌ها در بازارهای تبلیغاتی مرتکب تخلف می‌شوند و پول‌هایی به دست می‌آورند. مبارزه با تقلب برای شبکه‌های تبلیغاتی بسیار مهم است. به همین خاطر اکثر شبکه‌های تبلیغاتی و سایت‌های معتبر مانند گوگل، فیسبوک و هم چنین شرکت تبلیغات هوشمند تپسل سرمایه‌گذاری بسیاری در زمینه تشخیص تقلب در زمینه تبلیغات دیجیتال انجام داده‌اند.

با توجه به اینکه افراد متقلب دائماً در حال تغییر روش‌ها و تکنیک‌های خود هستند، فعالیت‌های آنتی فرد و مبارزه با تقلب کار ساده‌ای نیست.

در ادامه این بررسی به فعالیت‌هایی پرداخته می‌شود که شبکه هوشمند تبلیغاتی تپسل در این حوزه انجام می‌دهد.

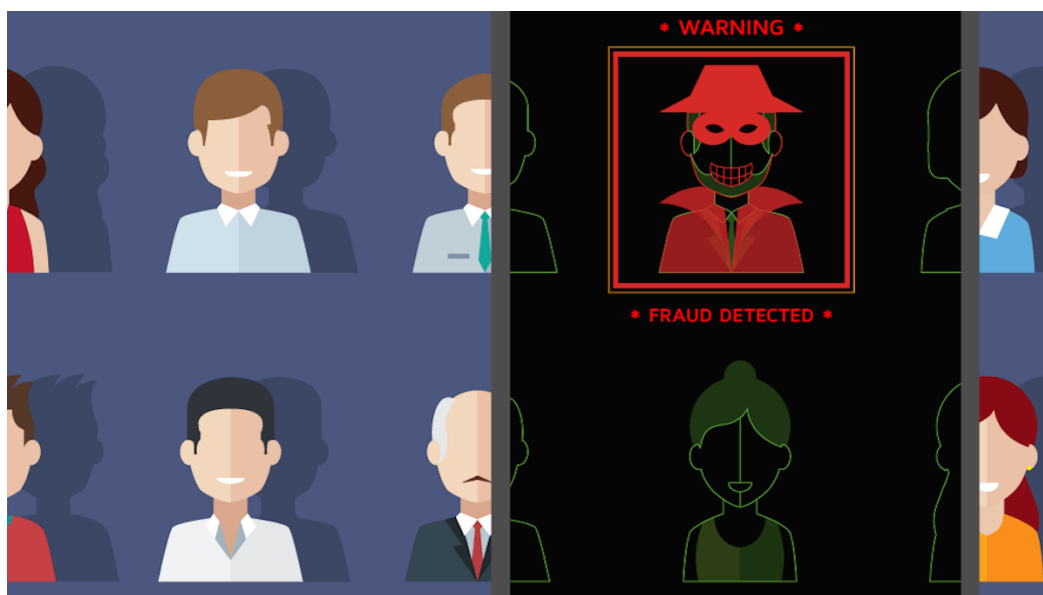
دستاوردهای تپسل در مبارزه با تقلب در تبلیغات

تیم تپسل تحقیقات و فعالیت‌های قابل توجهی در زمینه مقابله با تقلب‌های تبلیغاتی انجام داده است.

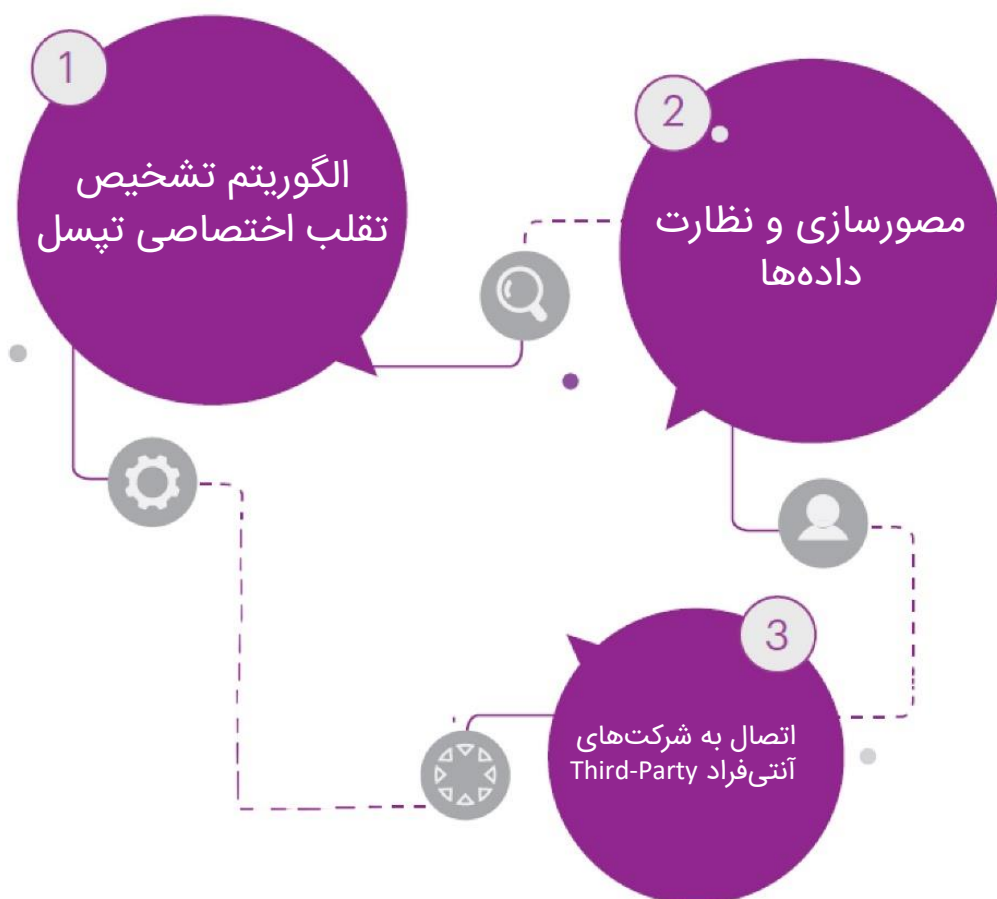
استراتژی تپسل، برای مقابله با تقلب، ترکیبی از تکنولوژی مورد استفاده در MMP ها و دیگر سرویس‌دهندگان تکنولوژی آنتی فراد است و با استفاده از آن‌ها راه حلی ترکیبی برای مبارزه با تقلب ارائه کرده است.

بنابراین به راحتی می‌تواند از سرویس‌های شبکه تبلیغاتی خود محافظت کند و این اطمینان خاطر را به مشتریان نیز بدهد.

با تشکیل تیمی برای آنتی فراد در تپسل و تلاش برای حفاظت از تبلیغات، کیفیت خدمات در این شبکه هوشمند تبلیغات قابل تضمین است. مجموعه تلاش‌ها و تکنولوژی‌های به کار رفته در این زمینه عبارتند از: استراتژی اختصاصی تپسل برای نظارت بر دیتا از طریق مصورسازی، الگوریتم تشخیص تقلب اختصاصی تپسل، تشخیص تقلب از طریق اتصال به شرکت‌های آنتی-فراد.



ما از این سه تکنولوژی در سیستم تشخیص تقلب تپسل استفاده می‌کنیم:



مصورسازی و نظارت بر داده‌ها

با توجه به سابقه تیم تپسل در کار با داده‌های مربوط به صنعت تبلیغات و شناخت معیارهای مهم در تعیین کیفیت ترافیک تبلیغات، این تیم توانسته است در طی زمان روشی جدید را برای مصورسازی داده‌های صنعت تبلیغات را به‌گونه‌ای ابداع کند که نظارت بر ترافیک‌های کانال‌های مختلف ساده‌تر شود تا از این طریق به راحتی بتوان تقلب را به صورت بصری تشخیص داد. علاوه بر این، با استفاده از ویژن به دست آمده از این مصورسازی داده‌ها نیز تپسل یک سیستم هشداردهنده ابداع کرده است که قادر است احتمال رخداد تقلب را تشخیص دهد و اطلاع‌رسانی کند.

الگوریتم تشخیص تقلب اختصاصی تپسل

پیاده سازی آنتی فراد به دو بخش تقسیم شده است. نظارت برخط (real time) و آنالیز آفلاین. برای قسمت ابتدایی، ۵ استراتژی به صورت موازی وجود دارد که می‌توان با استفاده از آن ترافیک نامعتبر را در همان زمان شناسایی و بلاک کرد. قسمت دوم بر اساس داده‌های پریودیک و متناوب که برای کانال یا ترافیک‌های ثبت شده، ویژگی‌های تقلب شناسایی و بلاک می‌شوند. تیم تپسل بر اساس نوع اپلیکیشن، استراتژی‌های مختلفی را در پیش گرفته است تا بتواند کارآمدترین مقابله با تقلب را داشته باشد.

تشخیص تقلب به صورت آفلاین | تشخیص تقلب آنی



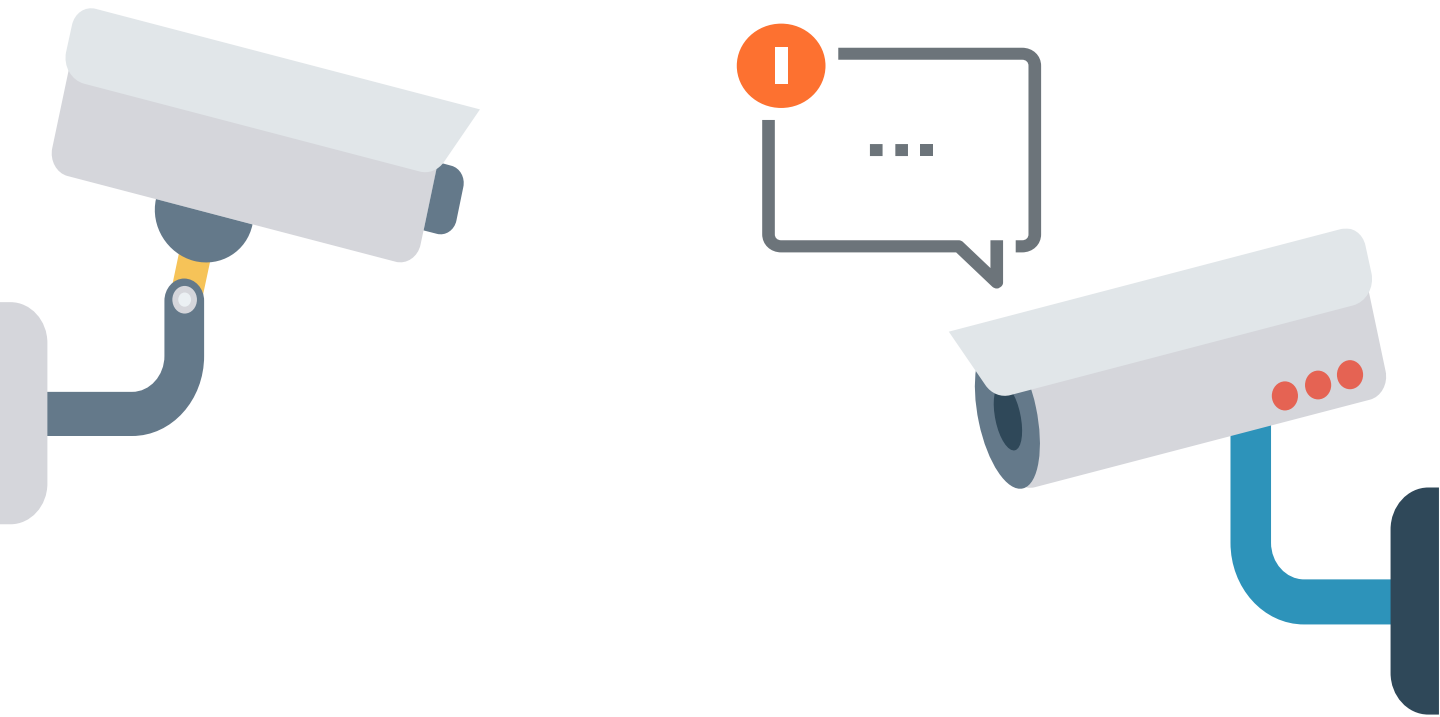
L تشخیص تقلب آنی

تشخیص برخط ناهنجاری

الگوریتم نظارت و تحلیل، همزمان رفتارهای کلیک مانند عدم مطابقت و یا ad stacking، در کنار بررسی ترافیک و کلیک‌های مشکوک به کار برده می‌شود.

فیلترینگ پویا

با استفاده از الگوریتم‌های تحلیل و شناسایی ترافیک و دیتایی که در تپسل تهیه شده است، فیلترینگ موارد نامعتبر به خوبی انجام می‌شود. مثلاً دستگاه‌هایی با رفتارهای غیرعادی و IP‌هایی که تقلب با آن‌ها شناسایی شده، به صورت پویا با فیلترها جدا می‌شوند.



تشخیص تقلب به صورت آفلاین

مدلسازی شاخص‌های آماری

از مدل‌های آماری و مبتنی بر یادگیری ماشین برای مدل کردن منابع متداول استفاده می‌شود، مثل CVR و یا تکرار IP و این مدل‌ها می‌توانند کل ترافیک‌ها را بررسی و تحلیل کنند، معیارهای غیرعادی بودن را پیدا کنند و به بهینه سازی ترافیک کمک کنند.

مدلسازی تحلیل و بررسی توزیع

با ترافیک‌های بالا، می‌توان دیتای موجود را در مدلسازی داده حجیم (big data) وارد کرد و می‌توان توزیع‌ها را بررسی و تحلیل کرد، مانند مدل دستگاه و مکان برای پیدا کردن ترافیک و یا زمان‌های غیر عادی.

مدلسازی رفتار کاربر

ما در تپسل بر اساس داده‌های رویدادها (از تبلیغ‌دهندگان) از روش‌های مبتنی بر یادگیری ماشین (جمع‌آوری اطلاعات و داده‌ها و تشخیص رفتار کاربر) استفاده می‌کنیم تا ترافیک مدلسازی شود و ناهنجاری‌ها پیدا شوند. این ناهنجاری‌ها شامل login، retention و بقیه مدل‌های رفتاری متداول می‌شود و البته محدود به این موارد نیست. با استفاده از آن می‌توان ترافیک تقلبی را شناسایی کرد.

روش مبارزه با تقلب با کمک Third Party ها

چنانچه پیشتر بیان شد، شرکت‌های مختلفی هستند که وظیفه آن‌ها تحلیل ترافیک‌های تبلیغاتی و شناسایی ترافیک واقعی و متقلبانه. با توجه به این که تپسل همواره به دنبال رساندن ترافیک تبلیغاتی باکیفیت برای مشتریان خود است، اتصال به این سیستم‌های تقلب‌یاب را از ابتدا در دستور کار خود قرار داده است و تا به امروز توانسته است با شرکت‌های مطرح در این زمینه هم‌چون adjust و Branch همکاری کرده و از سرویس آن‌ها در کنار روش ابداعی خود برای تشخیص تقلب کمک بگیرد تا تقلب را با دقت بالاتری تشخیص دهد.

به عنوان مثال، با توجه به اینکه SDK ترکرها در اپلیکیشن‌هایی که به دنبال تبلیغات نصبی یا CPA هستند قرار دارد، بنابراین ترکرها اطلاعات زیادی در مورد کاربرانی که اپلیکیشن‌ها را نصب می‌کنند دارند و می‌توانند تقلب را با دقت بالایی تشخیص دهند. علاوه بر این، با توجه به همکاری استراتژیک تپسل با این شرکت‌ها، در گزارش‌های مربوط به نصب‌ها که به تپسل داده می‌شود، اطلاعاتی در اختیار تپسل قرار می‌گیرد که می‌تواند از آن برای تشخیص دقیق‌تر تقلب استفاده کند و بدین‌ترتیب در صورتی که تقلبی وجود داشت که ترکرها قادر به تشخیص آن نبود، تپسل خود آن را شناسایی کند.

در سال ۲۰۱۷، روش SDK Spoofing یکی از روش‌های رایج تقلب در شمارش نصب‌ها شد و شرکت adjust نیز برای مقابله با این تقلب، SDK خود را آپدیت کرد. شما هم اگر در کمپین‌های تبلیغاتی خود در تپسل از adjust به عنوان third party استفاده می‌کنید، لازم است تا برای مصون بودن از تقلب‌هایی که در شمارش نصب در اثر کرک کردن نسخه‌های قدیمی SDK ادجاست اتفاق می‌افتاده است، نسخه SDK ادجاست موجود در اپلیکیشن خود را آپدیت کنید.





نتیجه‌گیری

تقلب‌های تبلیغاتی تا زمانی که کوچکترین انگیزه مالی برای متخلفین وجود داشته باشد، ادامه دارد.

خبر خوب این است که در حال حاضر تعداد زیادی شرکت برای مبارزه با آن شکل گرفته است. فقط در سال گذشته اتحادیه آژانس‌های تبلیغاتی آمریکا (4A's)، اتحادیه ملی تبلیغات (ANA)، مرکز تبلیغات متقابل (IAB) همه با هم، در جهت افزایش شفافیت و مسئولیت پذیری در صنعت تبلیغات، گروهی با عنوان پاسخگویی قابل اعتماد (TAG) تشکیل داده‌اند. TAG برای مقابله و از بین بردن تقلب در صنعت تبلیغات دیجیتال، حفظ امنیت محتوا و محصولات و حفظ یکپارچگی زنجیره فعالیت‌های دیجیتال مارکتینگ شکل گرفت و با هر شرکتی در زمینه فعالیت‌های تبلیغات دیجیتال همکاری می‌کند.

تپسل نیز به عنوان یکی از شرکت‌های فعال در زمینه تبلیغات دیجیتال، خود را متعهد می‌داند، که با تقلب‌های تبلیغاتی مقابله کند.

امید است که این راهنما گوشه‌ای از پیچیدگی مبارزه با آنتی فراد و تکنولوژی آن را آسان کرده باشد و نگرش درست و جامعی را در ذهن شما شکل داده باشد.



درباره تپسل

تپسل یک شبکه هوشمند تبلیغات دیجیتال است که با در اختیار داشتن شبکه گسترده‌ای از رسانه‌های دیجیتال و ارائه انواع مختلف تبلیغات بر روی این رسانه‌ها قادر است نیازهای تبلیغاتی بزرگترین برندهای تجاری از جذب کاربران باکیفیت برای اپلیکیشن‌های موبایل آن‌ها و یا عضویت آن‌ها در یک سامانه مشخص تا هدایت مشتری‌های هدف آن‌ها به وبسایت‌شان و همچنین برندسازی برای آن‌ها از طریق ویدئوهای تبلیغاتی را برآورده کند.

تپسل با استفاده از موتور پیشرفته مبتنی بر هوش مصنوعی خود قادر است علاقه‌مندی‌های کاربران خود را بشناسد و مرتبط‌ترین گروه کاربران را برای نمایش تبلیغ انتخاب کند و از این طریق تبلیغ‌دهندگان را قادر می‌سازد که با تپسل با کمترین هزینه به بیشترین ظرفیت تبلیغاتی دست یابند. علاوه بر این، سیستم پیشرفته تشخیص تقلب تپسل این امکان را در اختیار تبلیغ‌دهندگان قرار می‌دهد که تنها به ازای impression‌های واقعی هزینه کنند.

تپسل با در اختیار داشتن فضای تبلیغاتی برترین اپلیکیشن‌های ایرانی و خارجی به طیف متنوع و وسیعی از کاربران فضای دیجیتال دسترسی دارد و با استفاده از تیم مجرب و حرفه‌ای خود در زمینه تبلیغات توانسته است بزرگترین کمپین‌های تبلیغاتی را برای برندهای مطرح ایرانی و خارجی با موفقیت به انجام برساند. علاوه بر این، تپسل جریان درآمدی پایدار و قابل‌توجهی را بدون آسیب به تجربه کاربری برای صاحبان رسانه دیجیتال فراهم می‌کند و با بهینه‌سازی مداوم فضای تبلیغاتی خود، این امکان را برای صاحبان اپلیکیشن‌ها و وبسایت‌های موبایلی فراهم می‌کند که فضای تبلیغاتی رسانه خود را با بالاترین قیمت در تپسل به فروش برسانند و به eCPM بالایی دست یابند.



کالج تپسل، یکی از محصولات تپسل است که در سال 96 فعالیت خود را به صورت جدی آغاز کرد و هدف آن آموزش دیجیتال مارکتینگ به صورت رایگان است. کتاب الکترونیک حاضر نیز توسط کالج تپسل تهیه و تنظیم شده است.

دو کتاب الکترونیک دیگر در کالج تپسل منتشر شده است.





پازل مهارت‌های دیجیتال مارکتینگ خود را
با کالج تپسل تکمیل کنید!



www.tapsell.ir



info@tapsell.ir



[telegram.me/tapsell](https://t.me/tapsell)



[linkedin.com/company/tapsell](https://www.linkedin.com/company/tapsell)