HUMAN

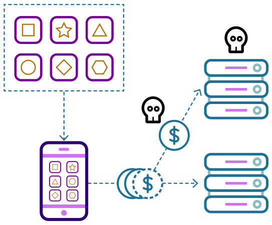
Marketing Fraud

Threats to Mobile Advertising

Mobile ad spend continues to grow. Though the industry's approach —with initiatives such as app-ads.txt— is having an effect, mobile fraud is still a billion-dollar industry. Given its size and complexity, fraud in mobile is even more significant than on other device types.

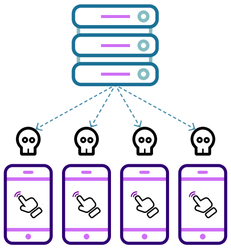
It's an ideal situation for fraudsters - high potential value, complex environments and low protective obstacles. The impact and cost of mobile fraud are high and can wreak havoc on a marketer's spend without ever knowing. Knowing is half the battle in the fight against fraud.

Mobile Fraud Threat Models



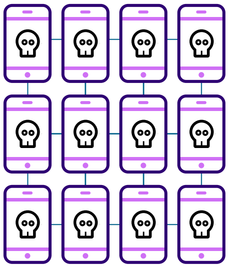
Fake Installs:

Attribution fraud from networks or affiliates using bots to derive false credit for installs they did not drive in order to earn the payouts.



Device Emulators:

Bad actors use data centers to create fake devices that look and act like humans while engaging with ads to steal install revenues.

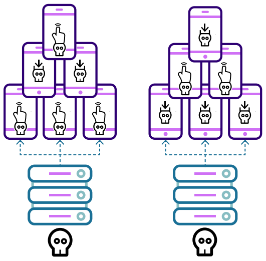


Device Farms:

Collection of actual physical devices run by bots to create fake user identities and actions that emulate human traffic. Similar to device emulators, they are compensated for installs.

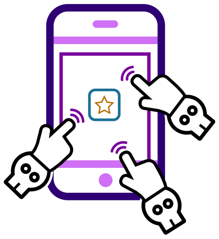
Device ID Reset:

Fraudsters reset mobile device IDs to allow for repeat installs of apps on the same device, each triggering a new device install credit to drive fraudulent install incentives payouts.



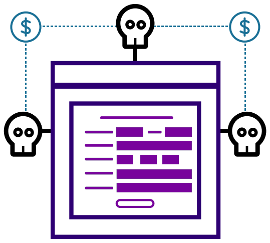
Mobile Attribution and Engagement:

Bot or device farm-driven installs and engagement sessions designed to fraudulently drive cost-per-engagement (CPE) payouts to malicious networks and app install affiliates.



In-App Click Generation:

Bots leverage advertisers' in-app advertisements to deliver credit for app opens and clicks inside the app to bad actors.

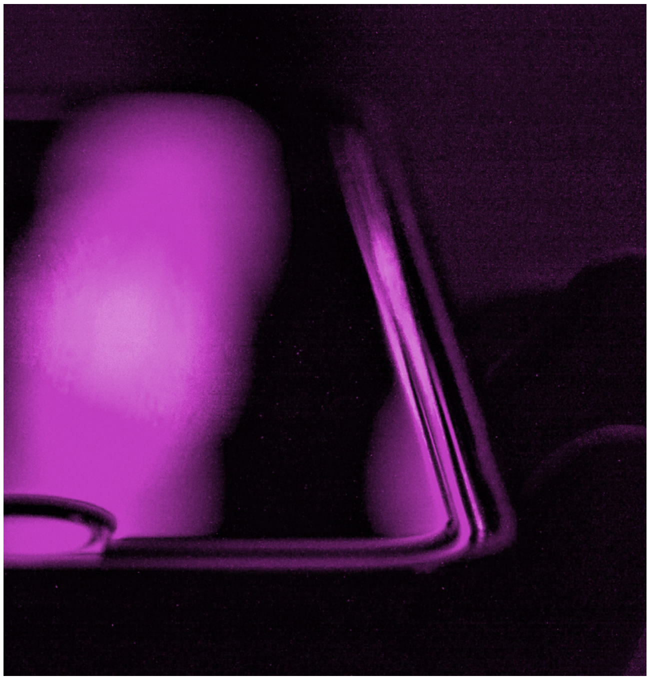


In-App Account Takeover and Abuse:

Bots that take-over user accounts using credential stuffing or credential cracking and perform fraudulent purchases and other fraudulent transactions or abusive interactions

Marketing Fraud

Threats to Mobile Advertising



Mobile Fraud Case Study

A global performance marketing agency noticed discrepancies with click rates that mobile install campaigns for clients across multiple download partners, known as affiliates. With HUMAN Marketing Integrity, the agency learned that several of the affiliates were contracting with sub-affiliates and publishers to deliver the campaigns. Several of these sub-affiliates were delivering a host of fraudulent clicks that were not tied to actual installs and stealing payouts for installs that never happened. **HUMAN helped the agency cut the fraudulent traffic sources, clean up the metrics and deliver verified human installs.**

About Us

HUMAN is a cybersecurity company that protects enterprises from bot attacks to keep digital experiences human. We have the most advanced Human Verification Engine that protects applications, APIs and digital media from bot attacks, preventing losses and improving the digital experience for real humans. Today we verify the humanity of more than 10 trillion interactions per week for some of the largest companies and internet platforms. Protect your digital business with HUMAN. To Know Who's Real, visit **www.humansecurity.com.**