The State of Mobile in Vietnam

-

Tony Wilcox
Director of Agency Alliances - APAC

HCMC - June 6th

AppsFlyer

AppsFlyer

THE ATTRIBUTION AUTHORITY

100%

Independent & Unbiased

4,600+

Integrated Partners

85k+

Applications

$19B

Ad Spend Measured

1T+

Mobile Actions Measured Per Month

AppsFlyer

Topics

1. 2019 Vietnam Insights and Benchmarks
    - Focus: E-commerce

2. Mobile Ad Fraud: A High Stakes Arms Race in Vietnam

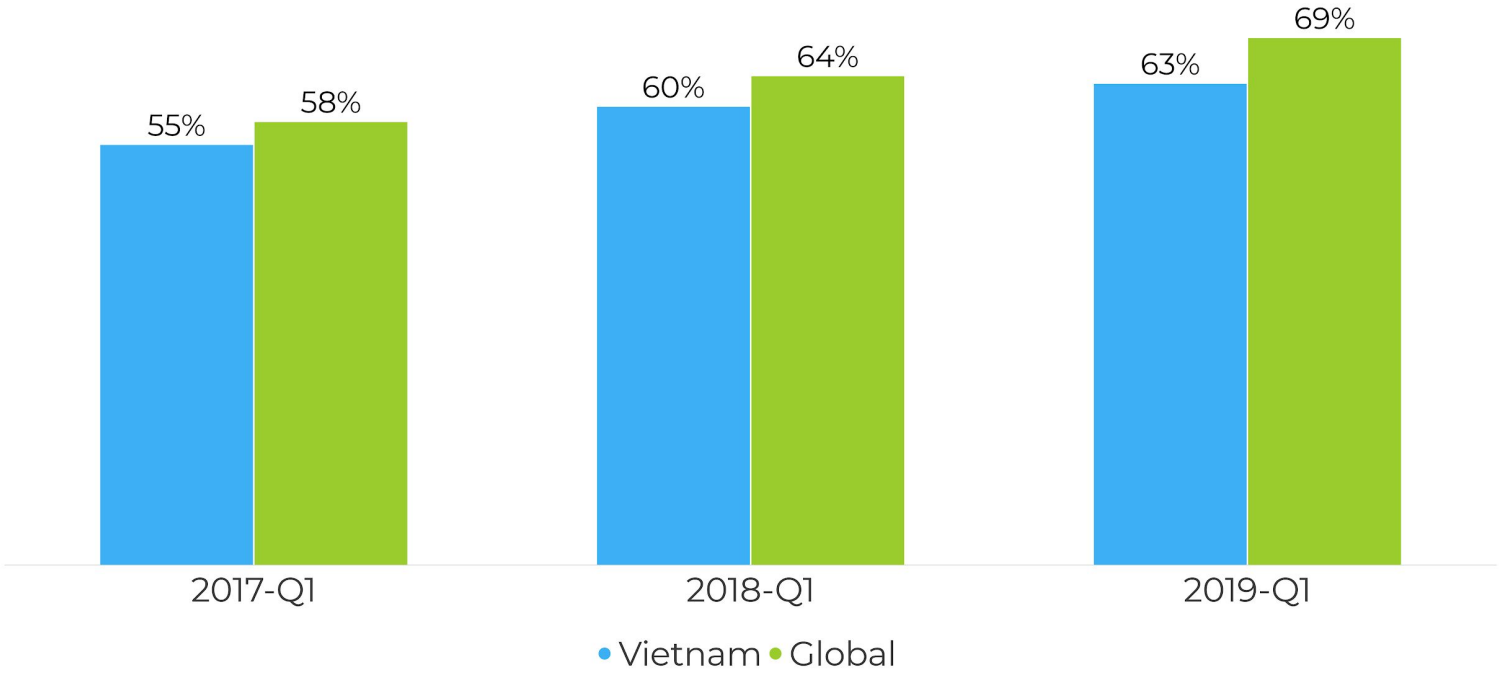
AppsFlyer

Chapter 1.

2019 Vietnam Insights and Benchmarks

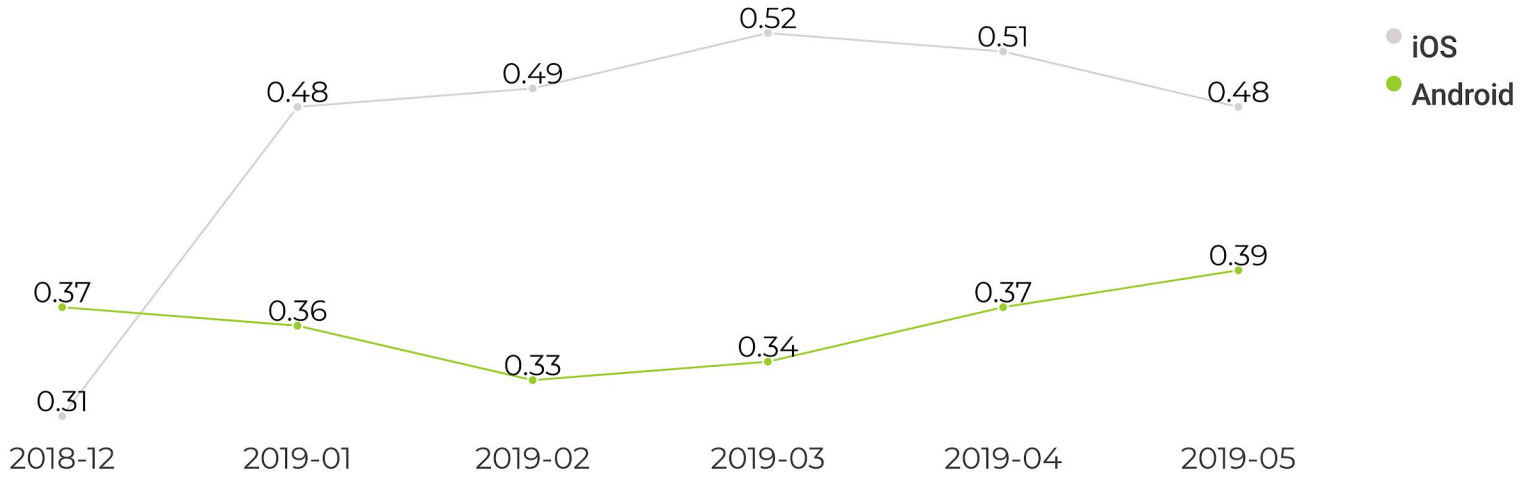
AppsFlyer

YoY Growth in Share of Non-organic Installs



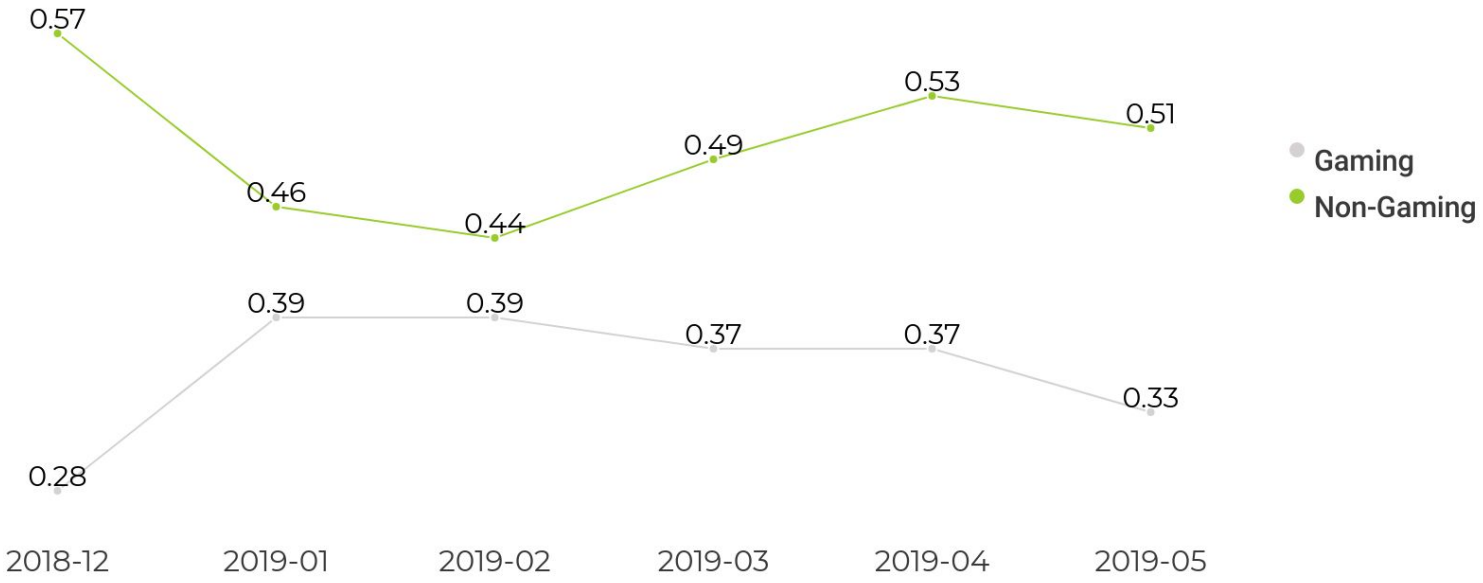
AppsFlyer

CPI Trend By Platform



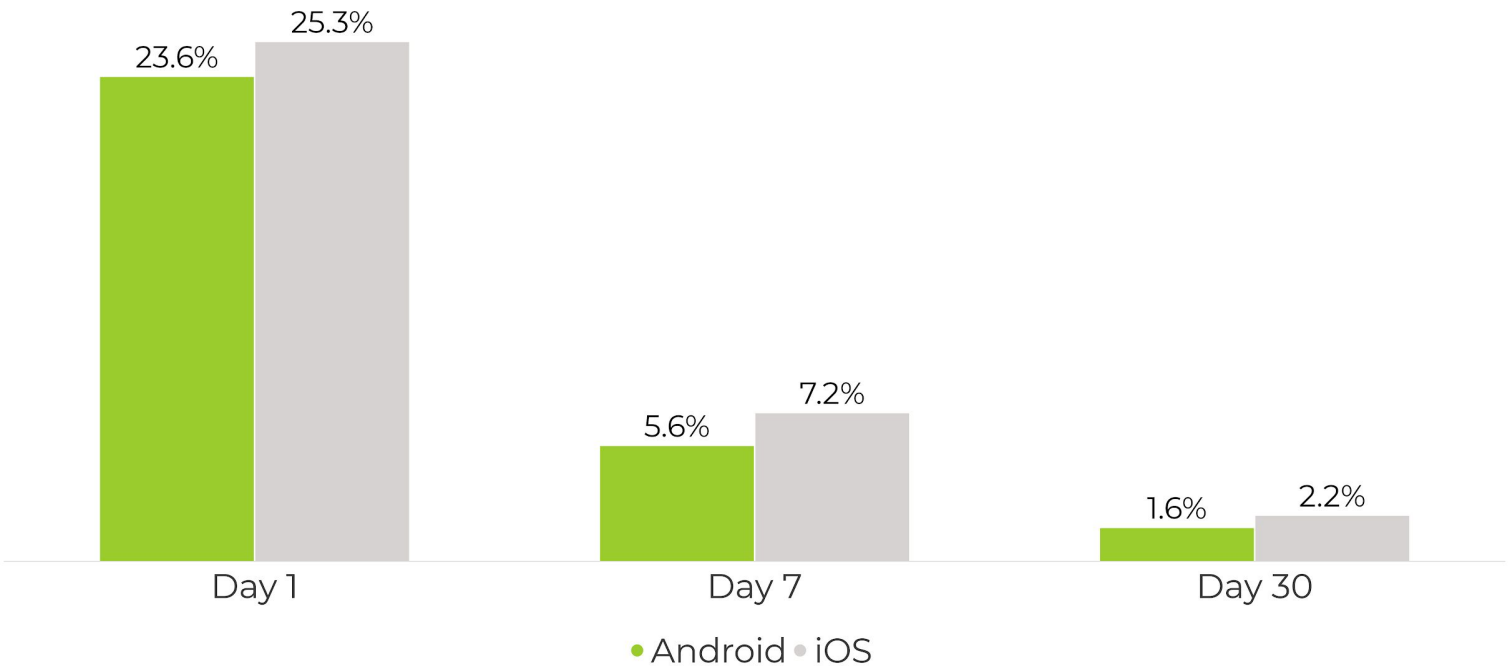
AppsFlyer

CPI Trend By Category



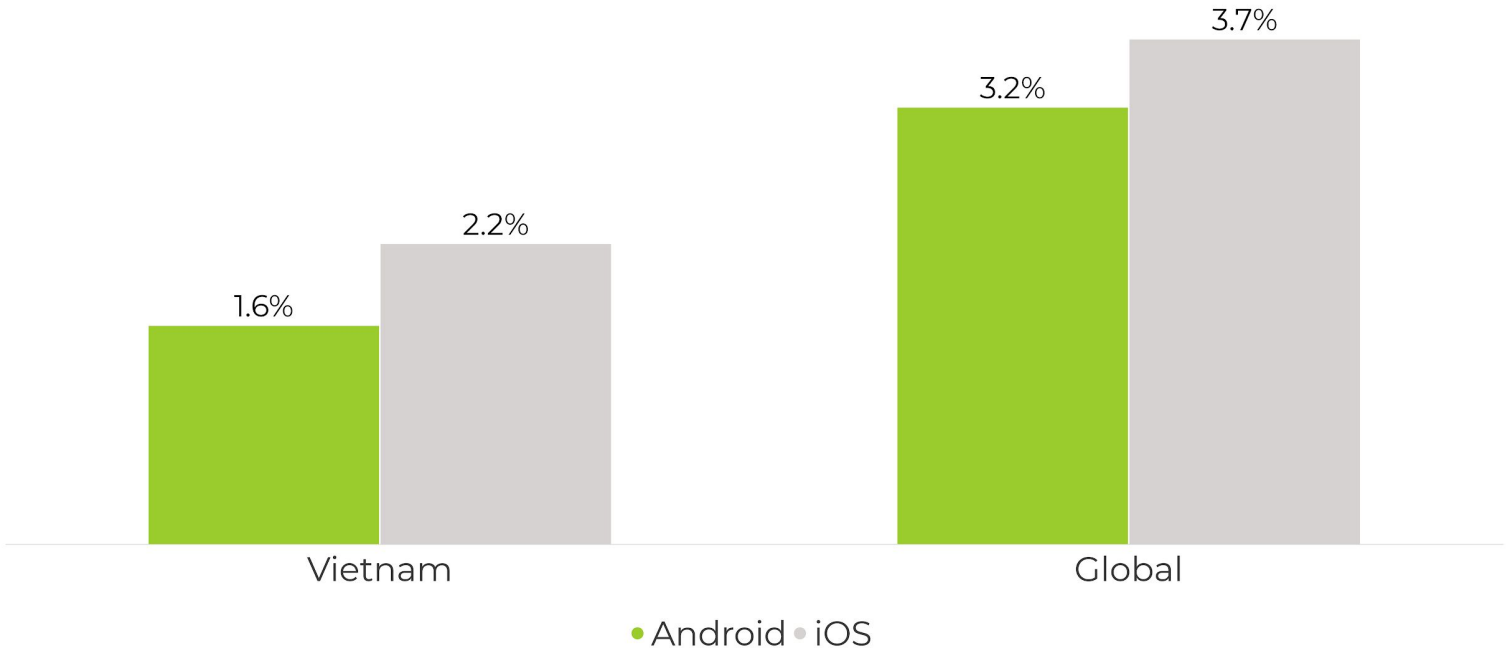
AppsFlyer

Retention Rate by Platform



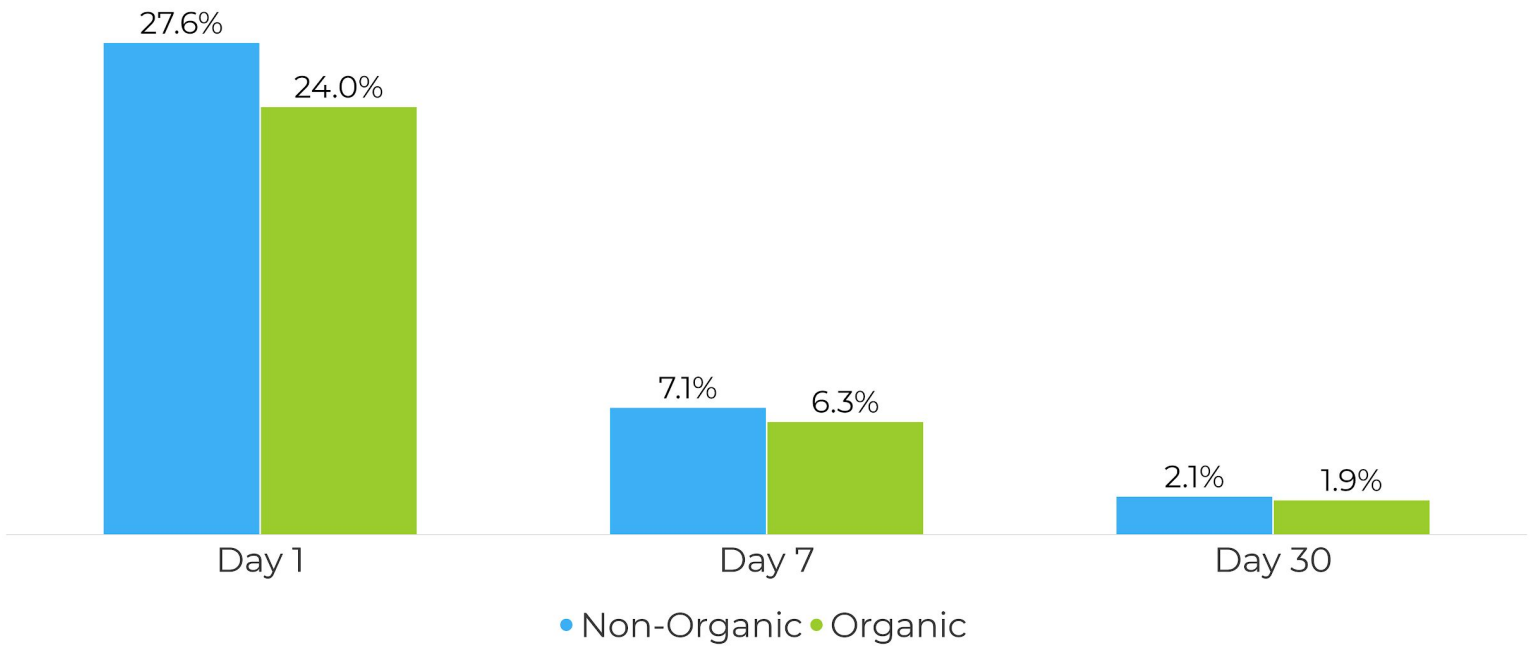
AppsFlyer

Day 30 Retention Rate by Platform



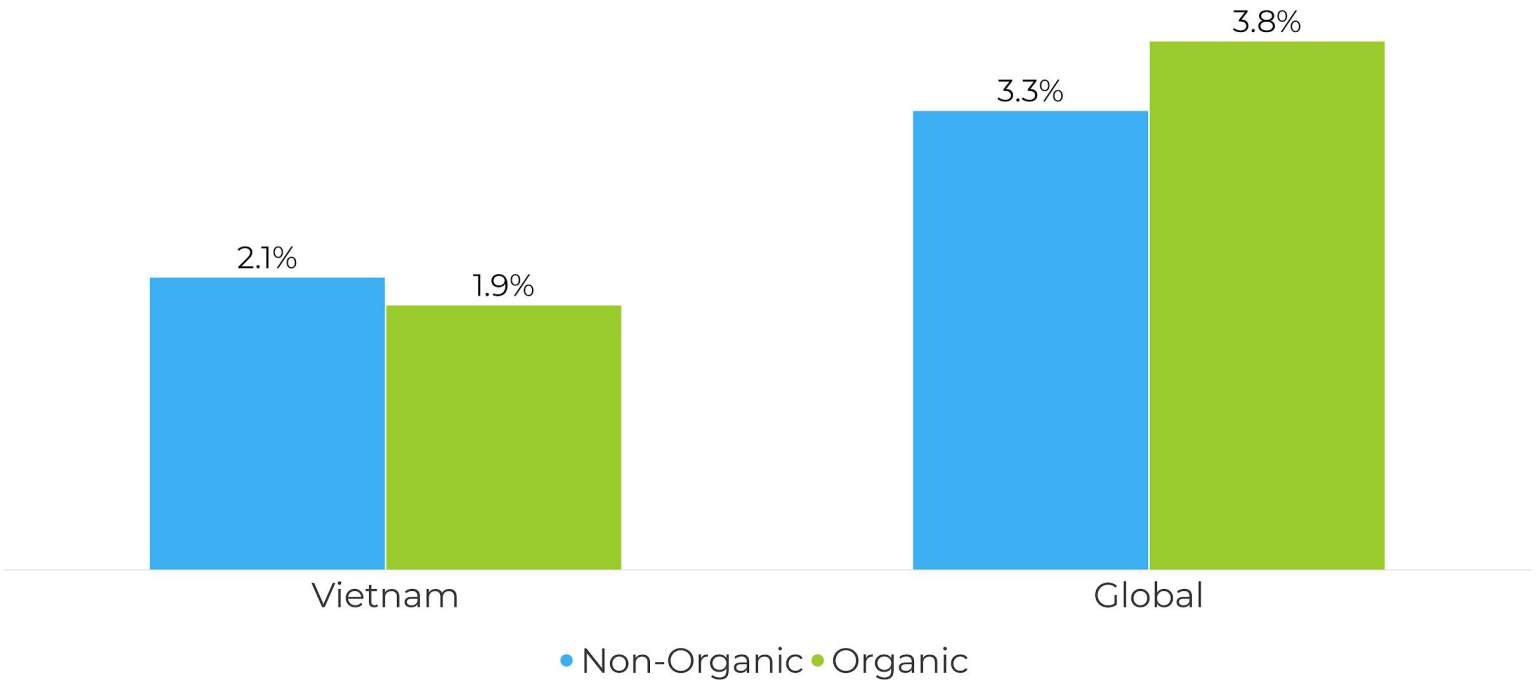
AppsFlyer

Retention Rate by Type



AppsFlyer

Day 30 Retention Rate by Type

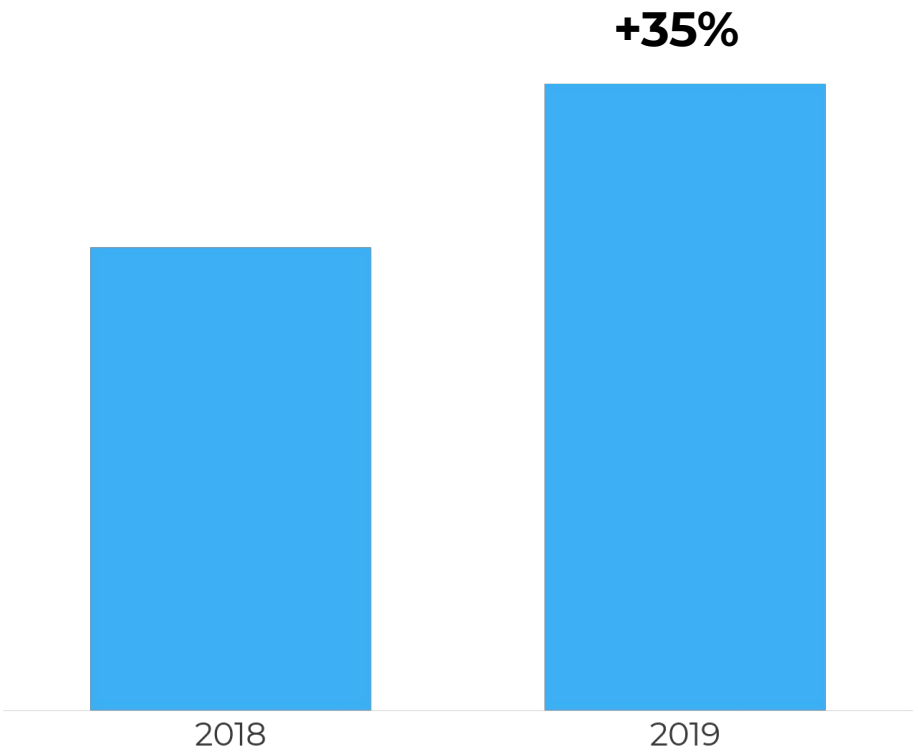


AppsFlyer

Focus:
E-commerce

E-commerce Retargeting Conversions

Q1 2019



AppsFlyer

E-commerce Retargeting Conversions

Among apps which had retargeting in 2018 and 2019

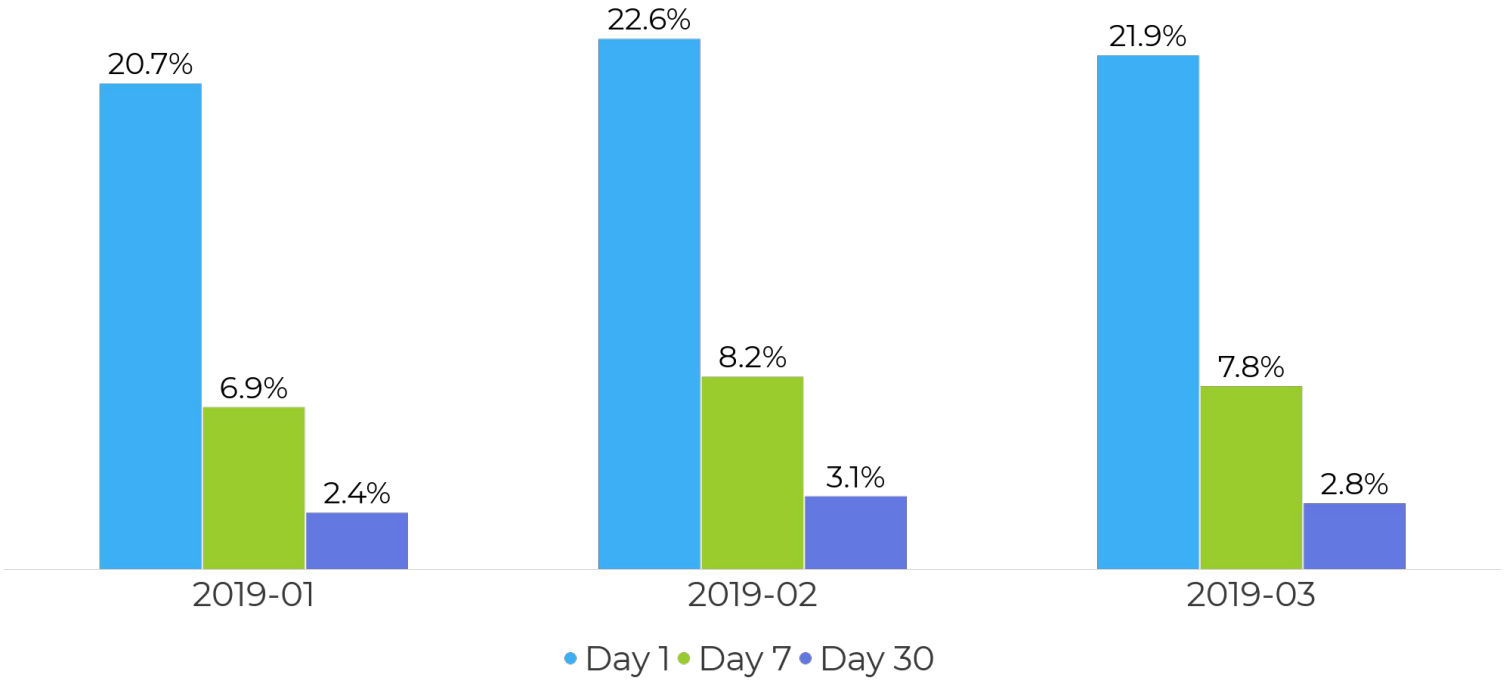
57%

had increased their retargeting conversions

AppsFlyer

E-commerce Retention Rates

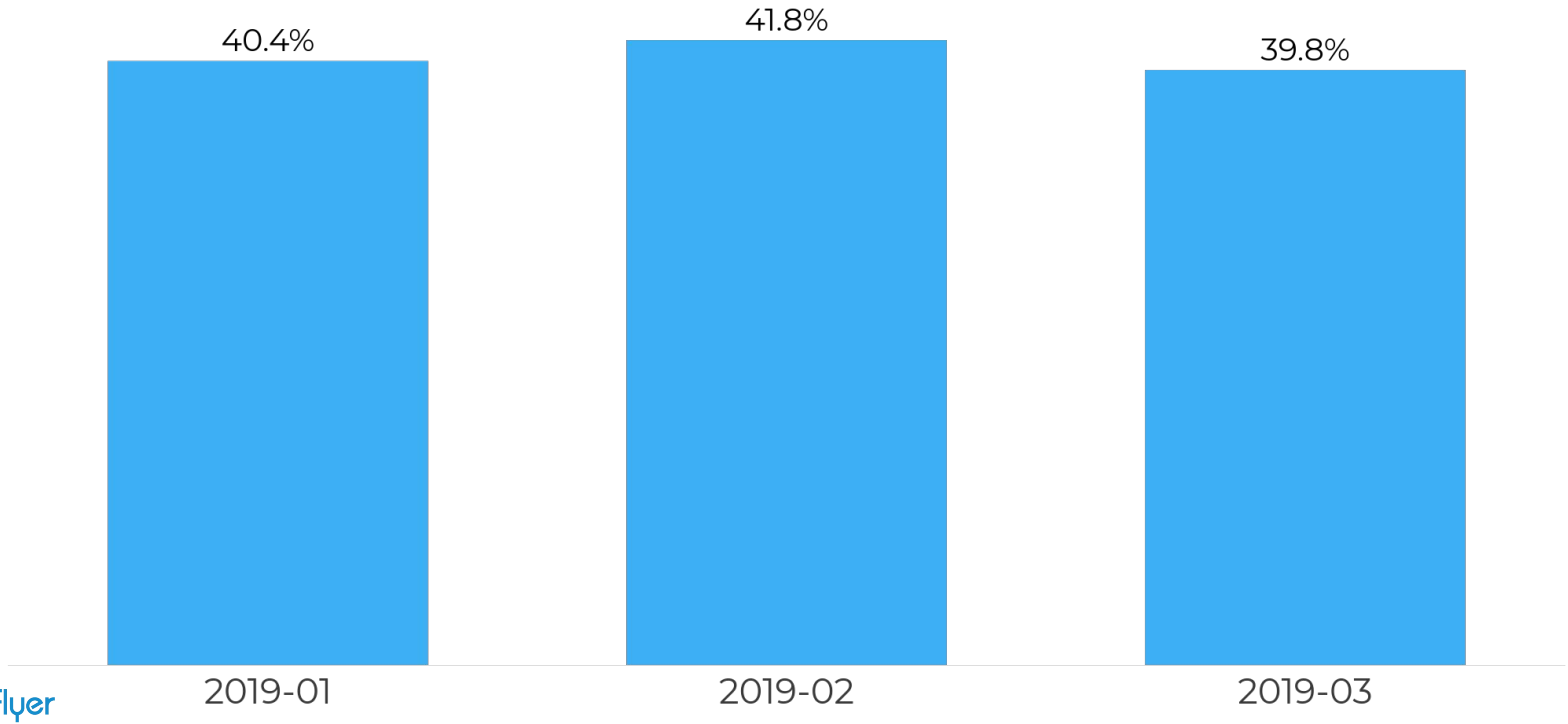
Q1 2019



AppsFlyer

E-commerce Uninstall Rates

Q1 2019



AppsFlyer

Chapter 2.

Mobile Ad Fraud **A High Stakes Arms Race in Vietnam**

AppsFlyer

AppsFlyer prevents

$6.7M

worth of fraudulent installs/day

AppsFlyer

Massive Increase in Financial Exposure

Estimated Global Fraud Exposure
Mobile App Marketing
(Q1 2019)

$450 - $550 MILLION

AppsFlyer

Source: AppsFlyer 2019, Q1

...Even in SEA

Estimated SEA Fraud Exposure
Mobile App Marketing
(Q1 2019)

$260
MILLION

AppsFlyer

Source: AppsFlyer 2019, Q1

The Impact of Mobile Fraud

23%

Fraud is Expensive

OF GLOBAL MOBILE MEDIA SPEND WASTED ON FRAUD

30%

Fraud is Pervasive

YEAR-OVER YEAR GROWTH IN COST OF MOBILE FRAUD ATTACKS

74%

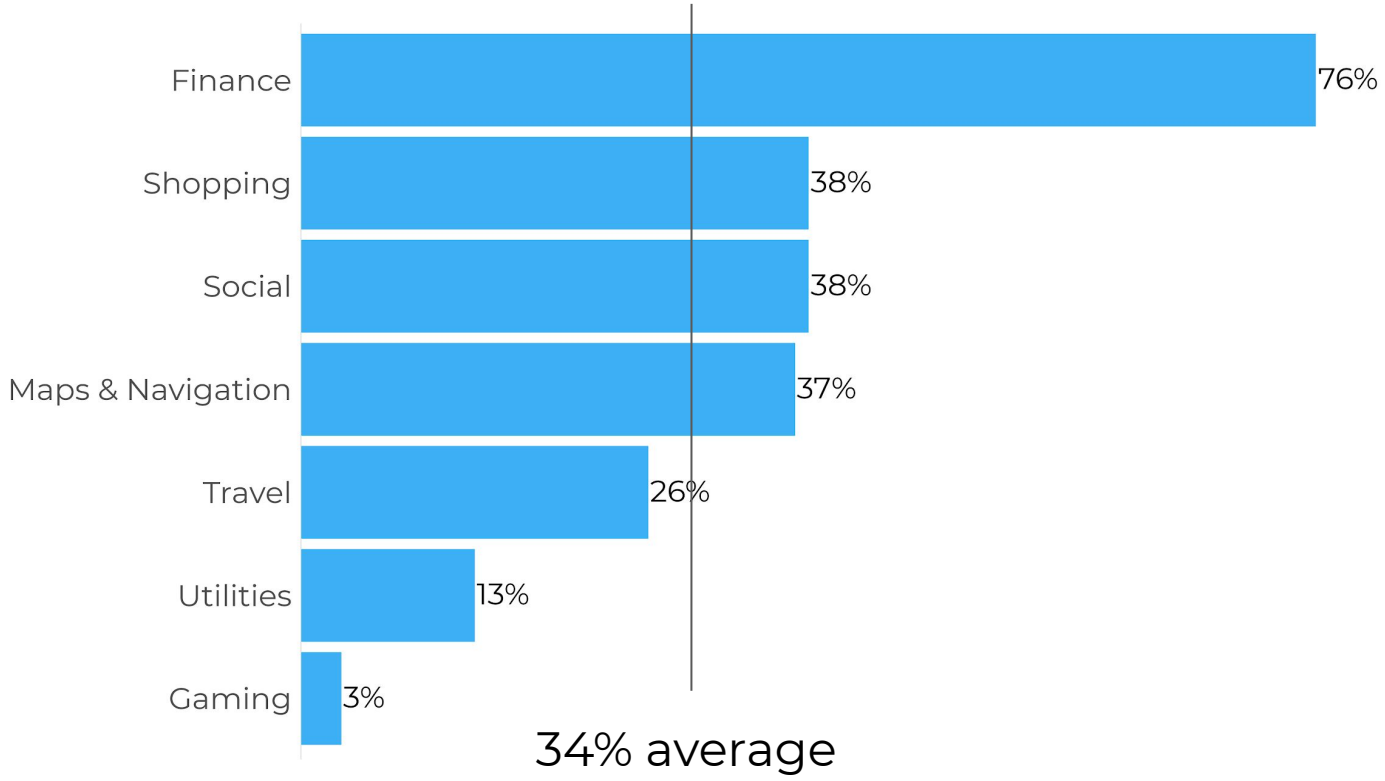
Fraud is Evolving

OF FRAUD IS PERPETRATED BY SOPHISTICATED AND SCALABLE FRAUD TACTICS

AppsFlyer

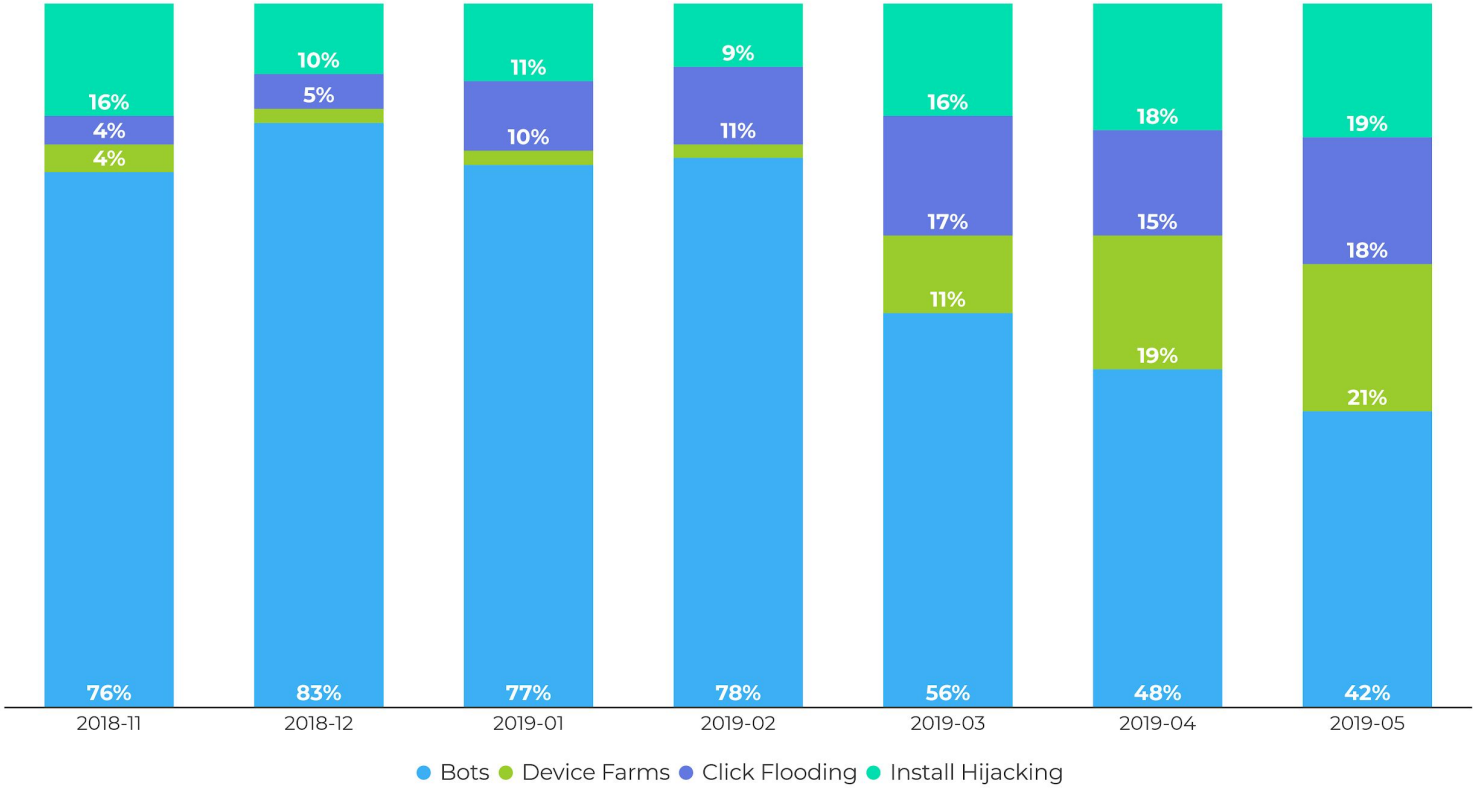
Source: AppsFlyer 2019, Q1

The not-so-secret fraud issue in Vietnam



Source: AppsFlyer 2019, May 2019

Fraud is evolving



Source: AppsFlyer 2019

What Fraud does to your business

Skews your App data

Eats your legitimate installs

AppsFlyer

The Bleeding Cash Cycle

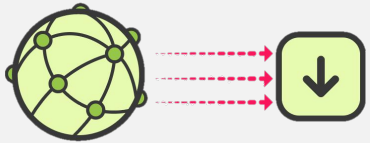
AppsFlyer

2 Main Types of Mobile Fraud

Attribution Hijacking

Install Hijacking/ Click Injection

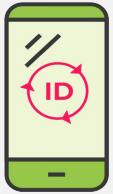
Activity Driven



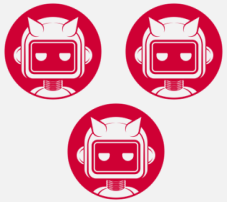
Click Flooding

Spray and Pray

Fake Installs



Device Farms



Bots

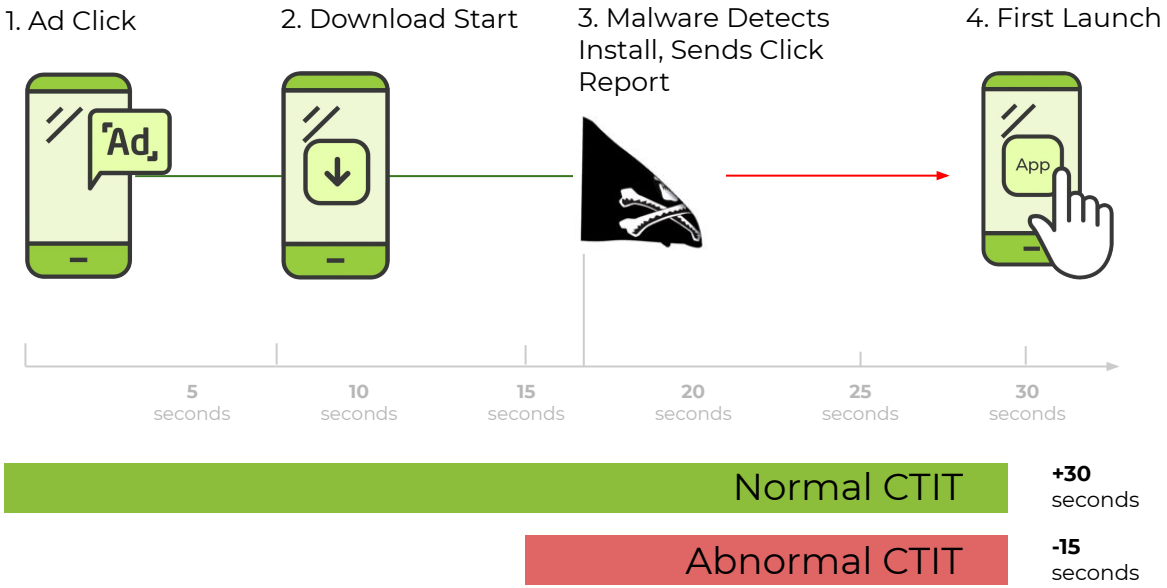
AppsFlyer

Install Hijacking

HOW IT WORKS

Install hijacking is a type of fraud where fraudsters “hijack” credit for an install.

Common techniques include sending false click reports or injecting false referrer data.



PROTECTION

Needs to use multiple signals including short CTIT, referrer mismatching, and multi-touch distribution patterns to identify and block install hijacking in real-time.

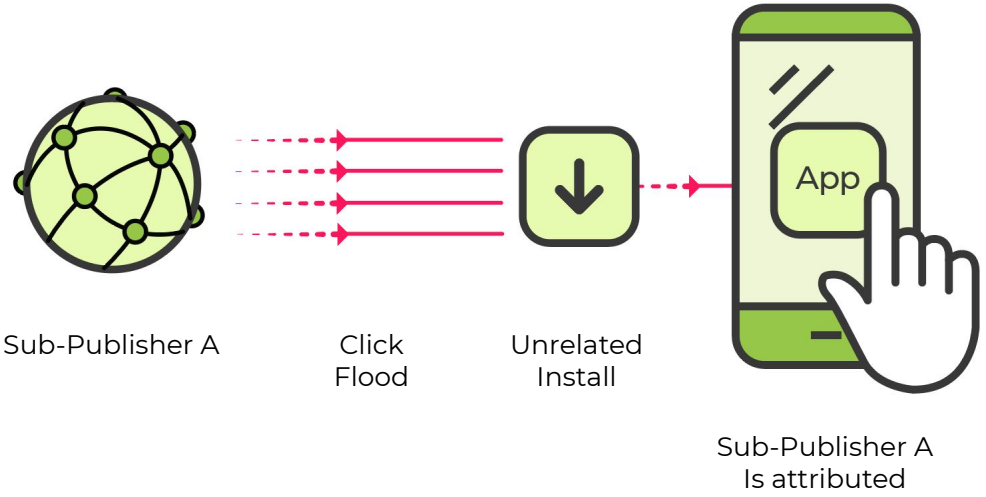
AppsFlyer

Click Flooding

HOW IT WORKS

In click flooding, fraudsters send a “flood” of false click reports from, or on behalf of real devices.

When the actual device downloads the app, the sub-publisher is falsely credited with the install.



PROTECTION

Needs to use signals including click-to-install time (CTIT), conversion rates and multi-touch contribution rates to identify and block click flooding at its source, in real-time.

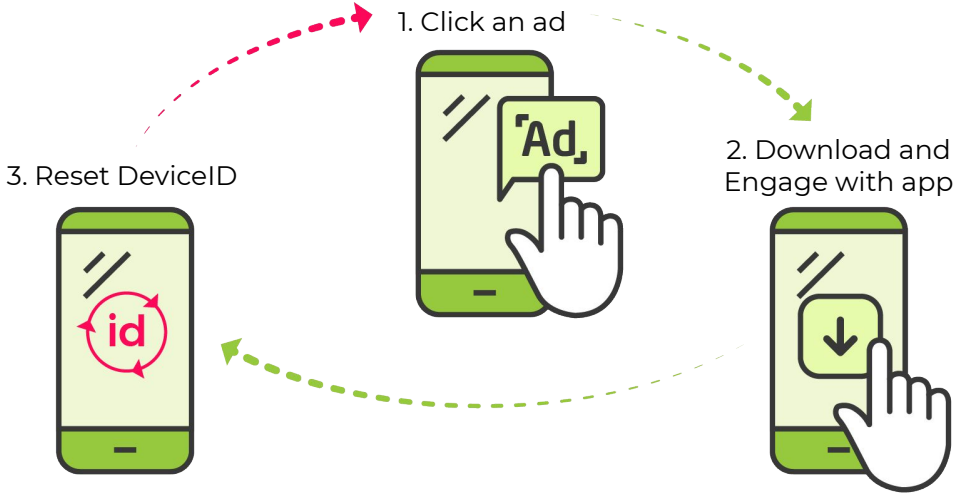
AppsFlyer

Device Farms

HOW IT WORKS

Device farms are locations full of actual mobile devices clicking on real ads and downloading real apps, hiding behind fresh IP addresses.

Over 2017, fraudsters started regularly resetting their DeviceIDs to avoid detection.



PROTECTION

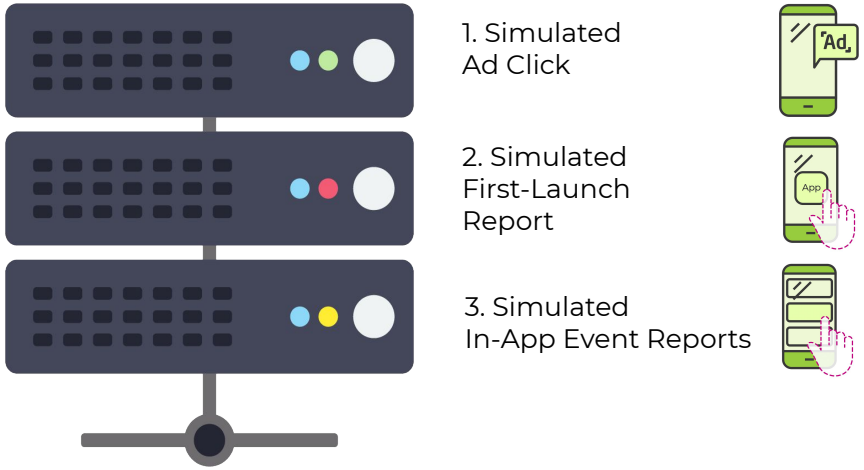
Needs to maintain active ratings for over 8.4 billion devices, automatically blocking device farms. Sub-publishers trafficking concentrations of devices “new” to the database are blocked in real-time.

AppsFlyer

Bots
HOW IT WORKS

Bots are malicious code that run a set program or action. While bots can be based on real phones, most bots are server-based.

Bots aim to send clicks, installs and in-app events for installs that never truly occurred.

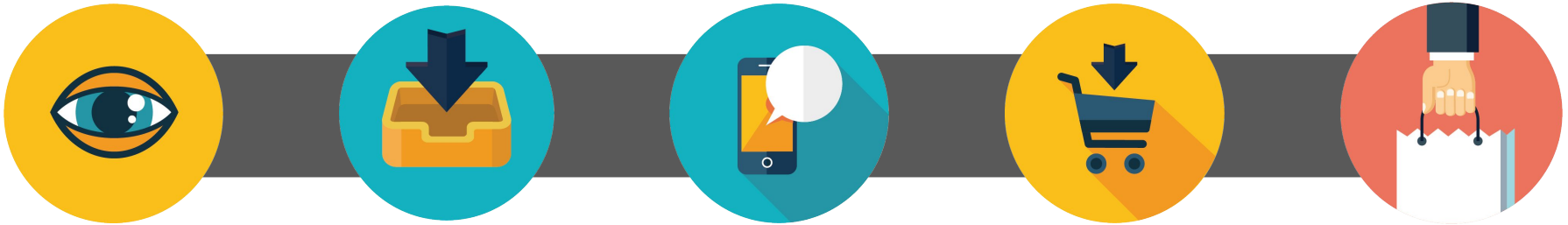


PROTECTION

AppsFlyer's unique data scale is able to identify both highly targeted and widely distributed bots operating at both lower and higher volumes, blocking bots in real-time.

AppsFlyer

Bots are becoming smarter



View/Click Install Browsing Add to cart Purchase

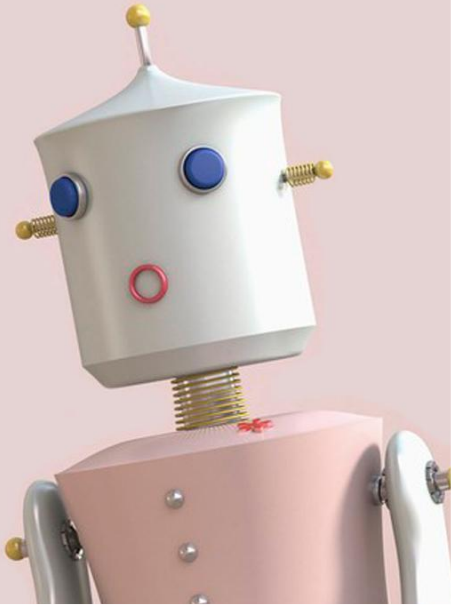
AppsFlyer

A simple bot recipe, part 1

Prep time: 1 day

Cooking time: Usually 30-60 days

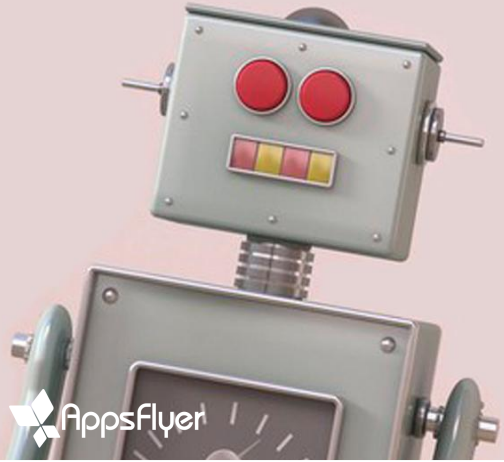
Ingredients:
- 1 Server
- 1 Attribution SDK, preferably open sourced
- 1 Anonymous IP package from the Darknet
- 1+ Ad network publisher accounts
- An abundance of device IDs



AppsFlyer

A simple bot recipe, part 2

1. Retrieve Ad URL
2. Create fake user agents
3. Mimic realistic in-app events
4. Randomize script behavior
5. Hide server location
6. Fire install & in-app events
7. Loop & Profit



AppsFlyer

Fraud prevention evolved

Fraud is more sophisticated and fraudsters often have multilayered methods, requiring a multilayered approach to effectively fight it

Device-level insights at scale

Comprehensive in-app event measurement

Machine-learning powered behavioral analysis

Layers of protection

AppsFlyer

Detecting fraud takes scale

$19 billion
Annual media spend measured

12 trillion
Annual in-app events measured

8.4 billion
Mobile devices carry AppsFlyer technology

Protecting Your Business

PROTECT360

30% Ad Spend Saved
1,000 Man Hours Saved Annually
20% Lift in ROI
25% User Base Growth

"AppsFlyer's anti-fraud solution, Protect360, saves our team a lot of time and delivers comprehensive mobile fraud protection, no matter the type."

Dyah Wulandari,
VP Performance Marketing

tiket.com

AppsFlyer

AppsFlyer