The Basics of App Fraud

Mobile fraud is a serious issue that is impacting the entire mobile ecosystem. We believe education is the first step in getting rid of this issue for good. We've created this guide to help our partners identify, and get closer to solving this problem faced by all mobile companies.

What is Install Hijacking?

This type of **mobile fraud** uses a **mobile malware** to **hijack attribution** for an **install. Install hijacking** is a broad category that includes the **"click injection"** as outlined below.

How Install Hijacking Works?

Click injection is a type of **install hijacking**. In click injection, malware on devices identify when the download process begins, and injects thousands of false click during the install process. This malware is often hidden in apps that looks to be legitimate.

1

The **banner directs** the user to the **App Store**

2

The user clicks the **download button** and the **app install begins.**

3

Click Injection

The **malware** identifies the **download process** and **injects false clicks.**

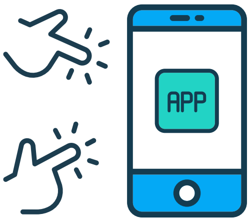
4

The **download is completed**, the user opens the app and the **tracker receives** the **data from the install.**

5

The **install** is **attributed** to the **last click** that the **malware** made and the **tracker** will **identify** it as **fraud**.

The Basics of App Fraud



What is Click Spamming or Click Flooding?

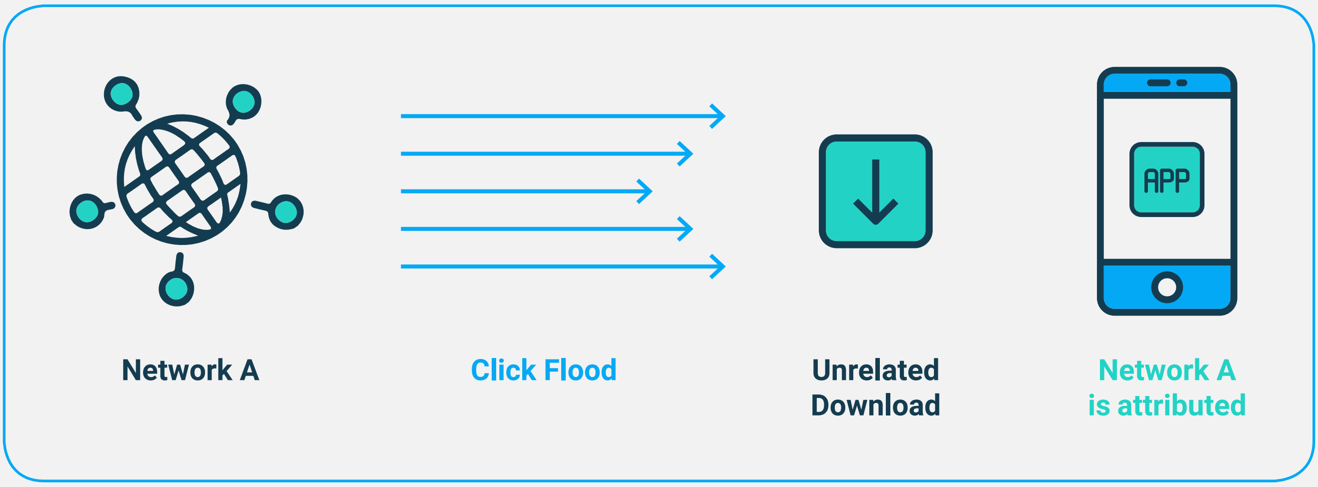
Click Flooding, also known as click spamming, is a type of mobile fraud where networks send large numbers of fraudulent clicks to deliver the last-click prior to installs.

How to prevent Click Spamming?

We recommend using the metric **Click to Install Time (CTIT)** along with a cohort analysis to detect and proof Click Fraud. CTIT analysis the first 2 to 24 hours, as well as between days 2 and 7 after install. To measure and detect CTIT and any time-based parameter, we recommend to use timestamps to determine it.

- **Conversions** delivered **60 minutes after the click** will be considered **highly suspicious** since normally less than 35% occur in that range of time.
- **Media Sources:**

  CR below **0,05%** will be considered **fraud.**
  CR below **0,3%** will be considered **highly suspicious.**


Network A
Click Flood
Unrelated Download
APP
Network A is attributed