# Mobile ad fraud: Frauds leading to fake app install and engagements

In click spamming an indefinite number of clicks are used whereas in click injection, a single click is used at the time of download. It specifically targets Android-based devices.

This ad fraud starts when the user downloads or installs a new app, fraudsters get a notification through an Android broadcaster, and they trigger a fake click at that precise moment before the download is complete. This injected click gives them access to the user's device tracking code, making the click seem genuine.
This ad fraud starts when a user lands on a page or downloads an app operated by fraudsters. The moment the app is downloaded, the fraudsters start generating massive fake clicks on the app which continues to run in the background, of which the user is unaware. Most of the time, it looks like the user interacts with the ad whereas they don't even see it.

Read more about Frauds leading to fake app installation and engagements