FRAUD ALERT!

CLICKFRAUD APPS!

India Today (7th Dec 2018) - Google deletes 22 Android apps with hidden virus, check this list to see and ensure they are not in your phone.

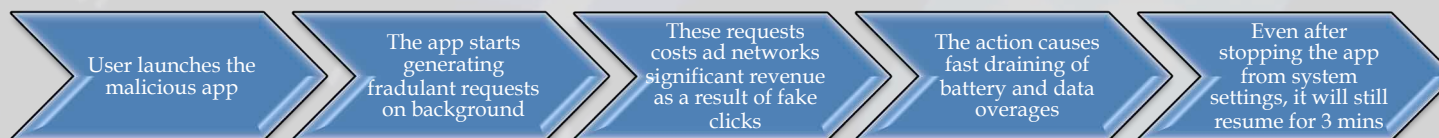**As far as the 22 apps that you should not have on your phone:**

1. Sparkle FlashLight
2. Snake Attack
3. Math Solver
4. Shape Sorter
5. Tak a Trip
6. Magnifeye
7. Join Up
8. Zombie Killer
9. Space Rocket
10. Neon Pong
11. Just Flashlight
12. Table Soccer
13. Cliff Diver
14. Box Stack
15. Jelly Slice
16. AK Blackjack
17. Color Tiles
18. Animal Match
19. Roulettta Mania
20. HexaFall
21. Hexa Blocks
22. PairZap

What is ClickFraud App?

Mobile platform fan-favoritism aside, there is a distinct difference between the worlds of Android and iOS mobile devices: Advertisers will pay a premium to reach the supposedly deep-pocket owners of Apple phones and tablets. As clickfraud grows as a revenue stream for unscrupulous mobile app developers, it turns out that it pays well to lie about what kind of mobile device is fraudulently clicking those ads.

How Most of the ClickFraud Apps Work?

User launches the malicious app	The app starts generating fradulant requests on background	These requests costs ad networks significant revenue as a result of fake clicks	The action causes fast draining of battery and data overages	Even after stopping the app from system settings, it will still resume for 3 mins

Impact on End Users?

From the user's perspective, these apps drain their phone's battery and may cause data overages as the apps are constantly running and communicating with servers in the background. Furthermore, the devices are fully controlled by the command and control (C2) server and can potentially install any malicious modules upon the instructions of the server.

Stay Safe

- Do not download unnecessary apps in your smart phones.
- Necessary apps to be downloaded from reliable sources only.
- Avoid downloading apps through links sent on email or messages.
- Delete all unnecessary apps immediately OR deactivate them from system settings