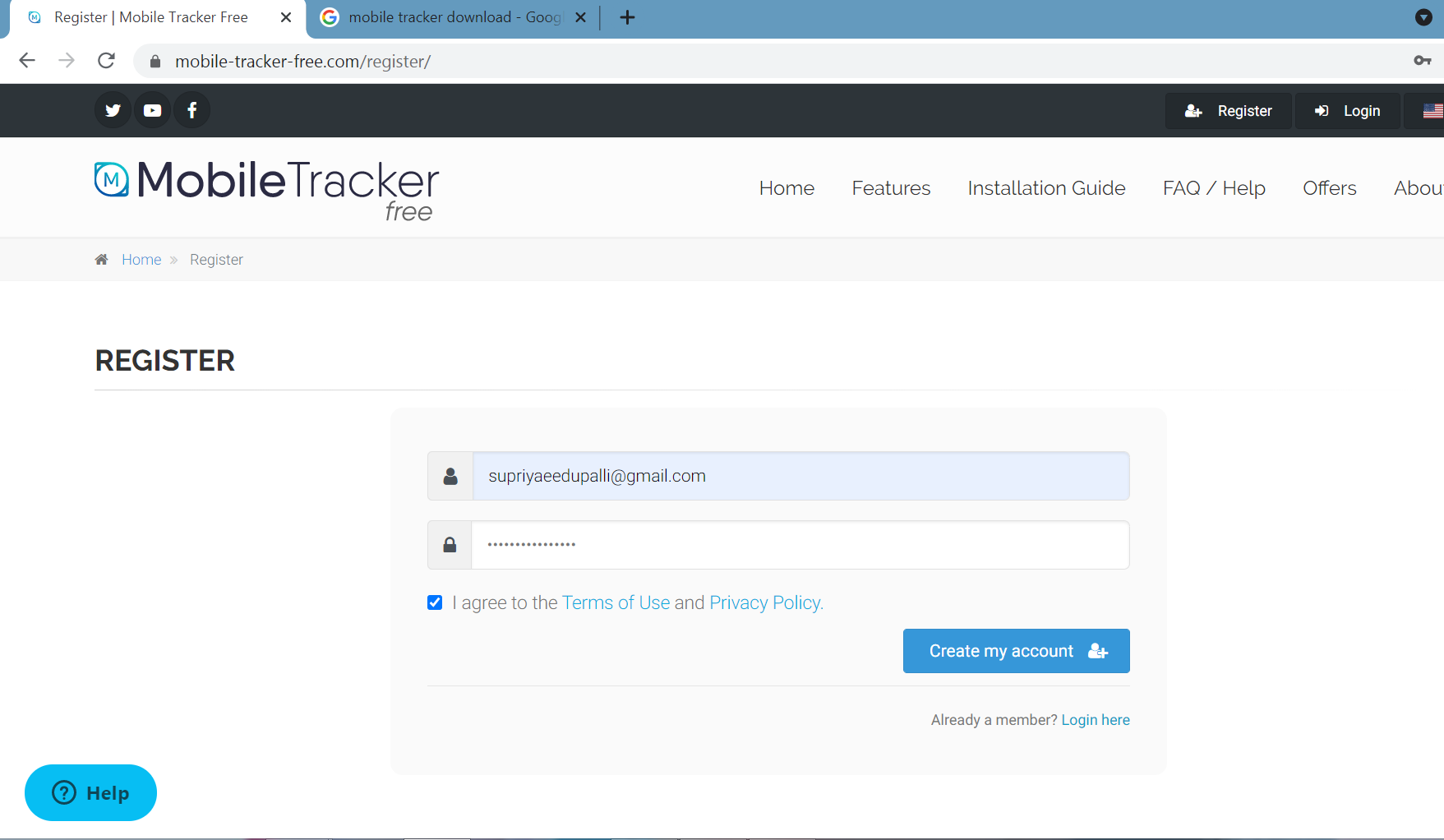
**PROBLEM STATEMENT:**

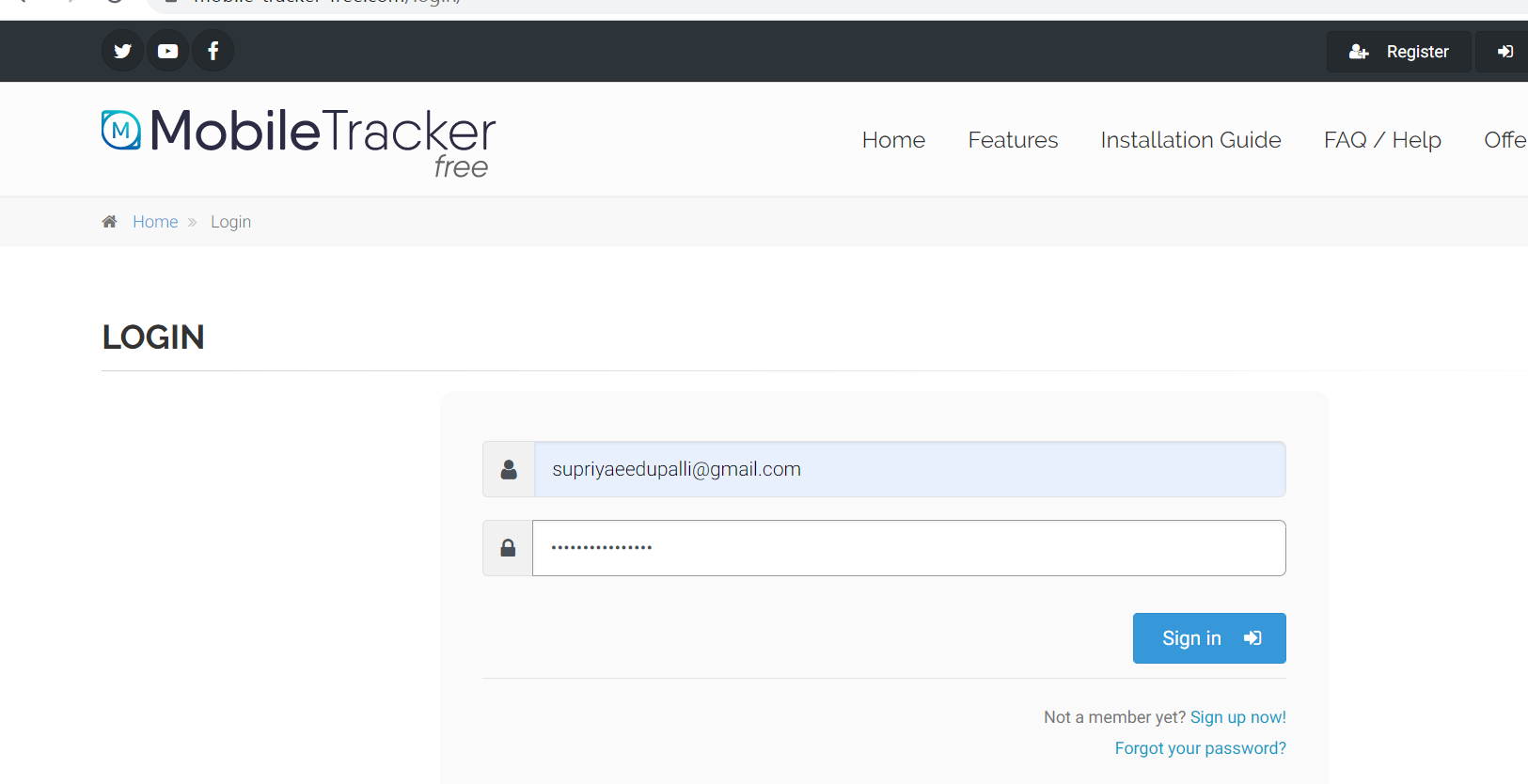
6. Use Mobile tracker free (online tool) to install in android mobile phone and try to execute the commands and taken live webcam stream and screenshots and whatsapp messages. Write a report on that attack and provide solutions to avoid android hacking .

**SOLUTION:**

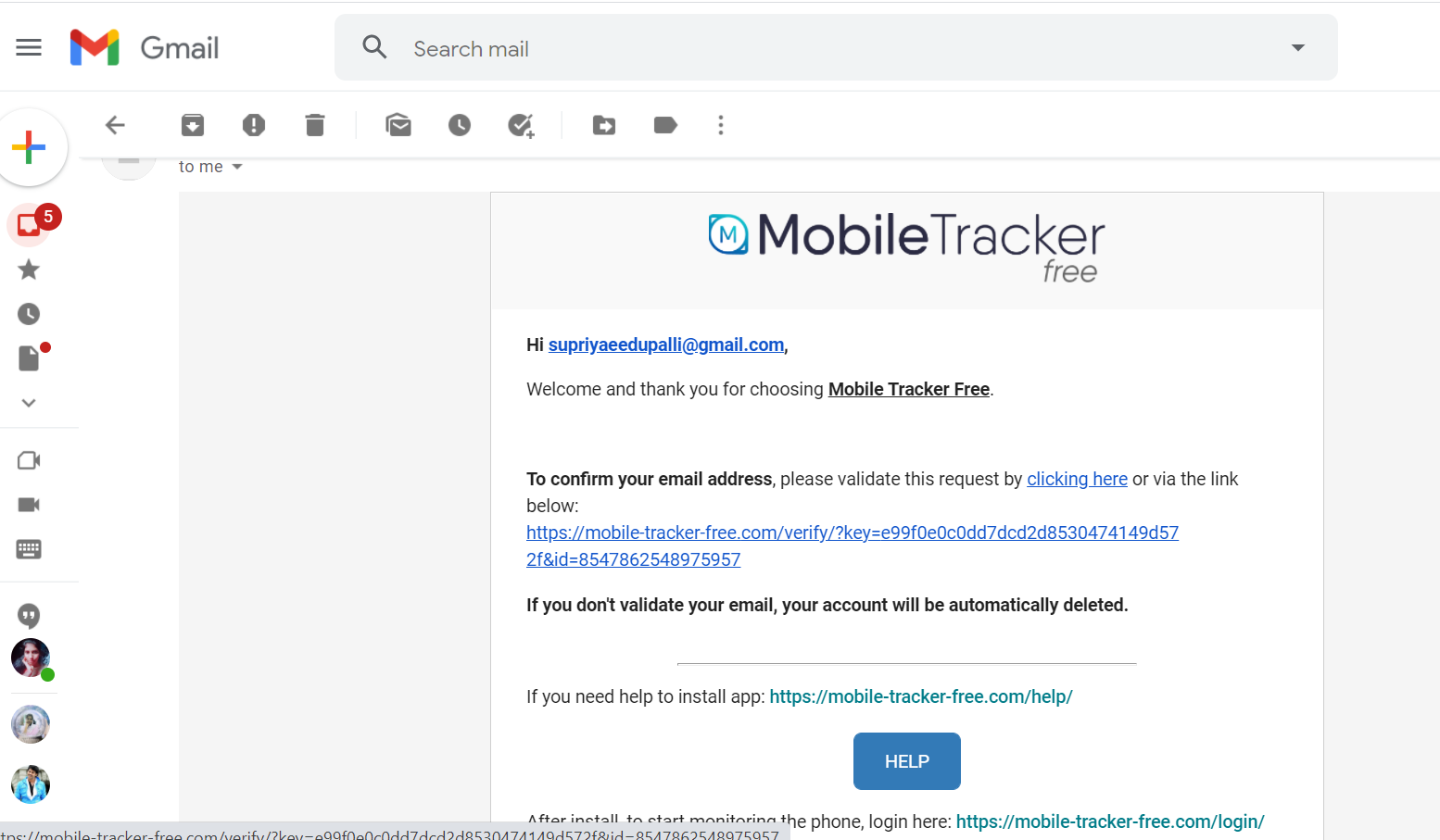
1. **First register on the mobile tracker website.**

****

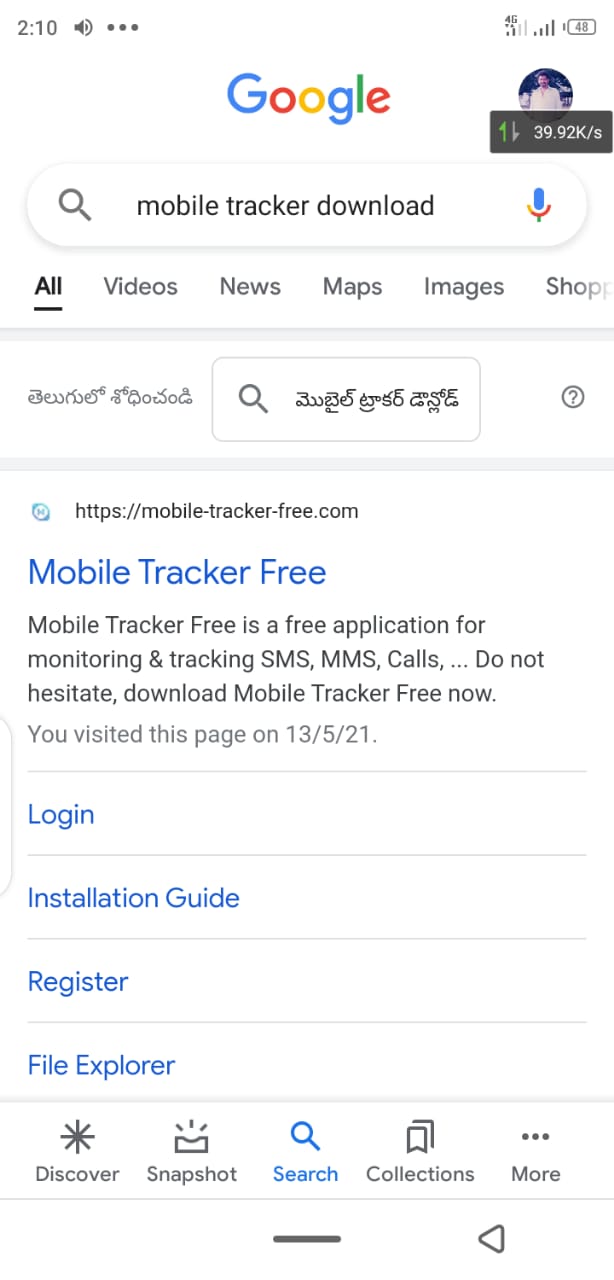
1. **Login the same email id and password.**

****

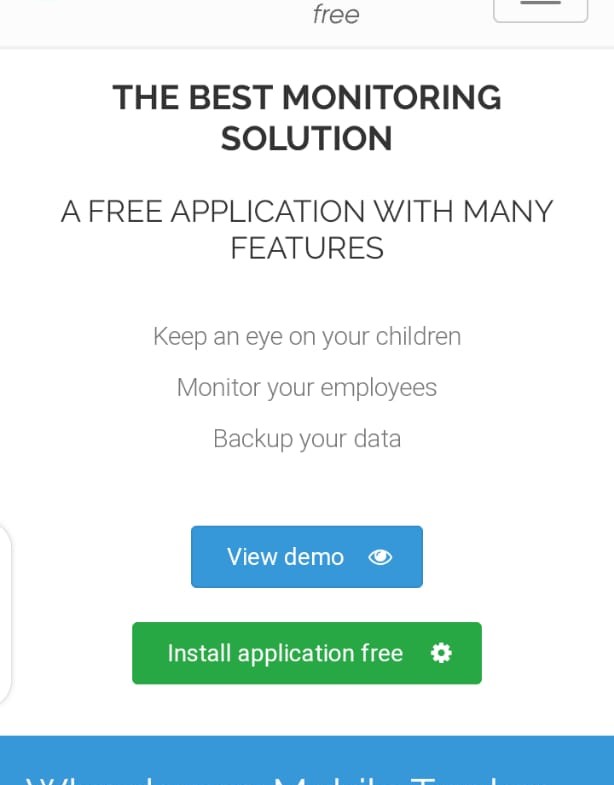
1. **We check the given gmail,it gets the link.click on the link .Your account will be activated.**

****

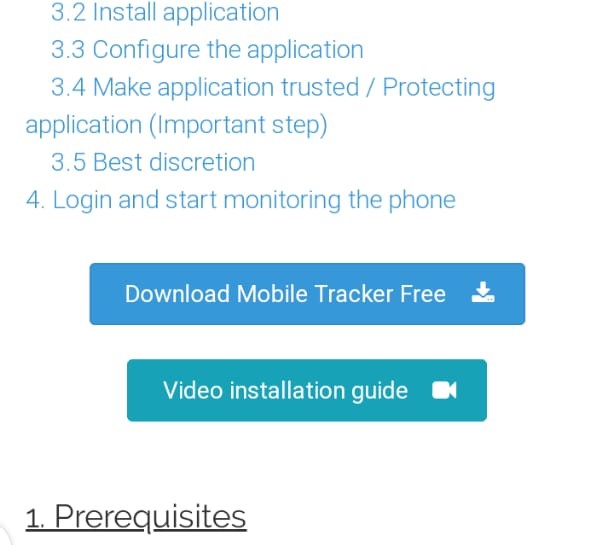
1. **Open the web browser and search on the mobile tracker download.**

****

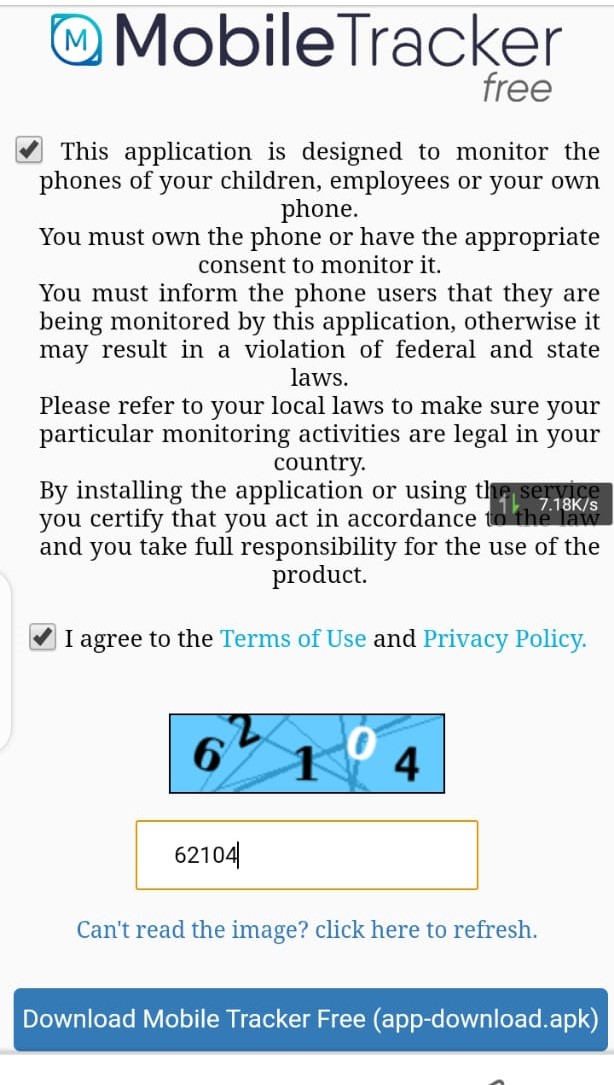
1. **Install the application on mobile hacker.**

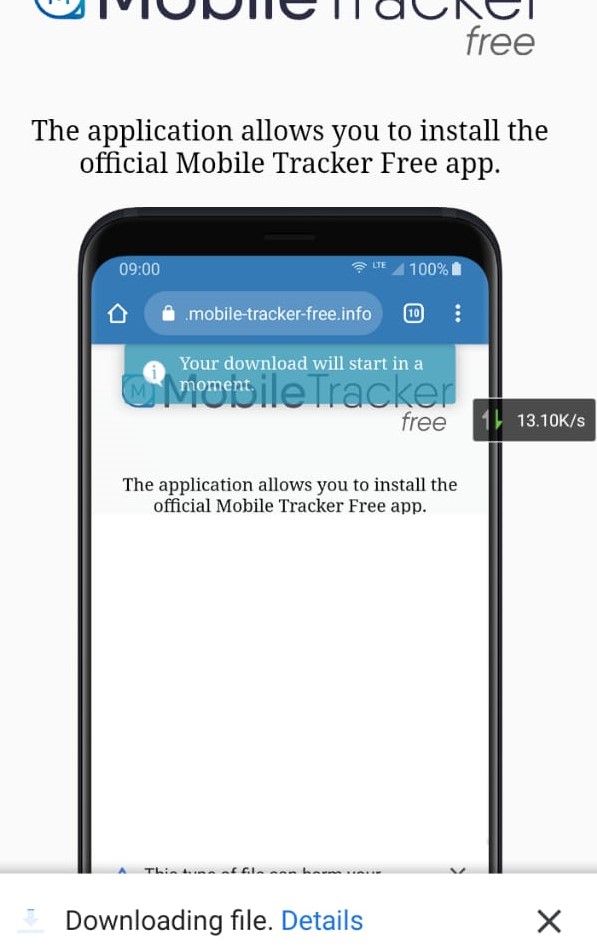
****

1. **Download the mobile hacker tracker free.**

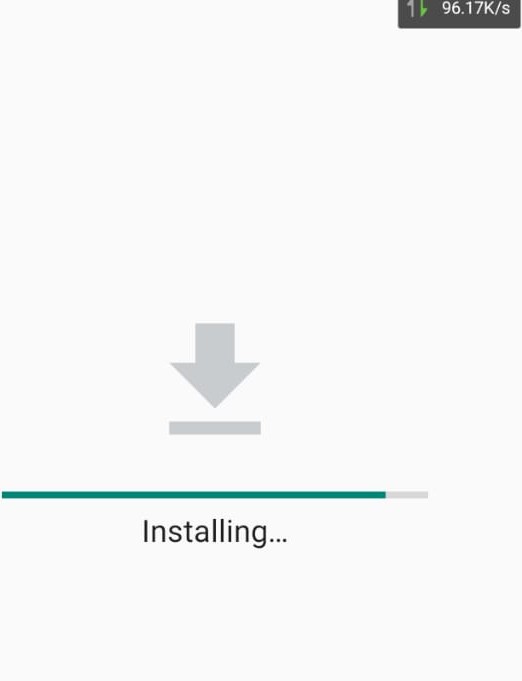
****

1. **Click on the i agree And Capture the code,click on download mobile tracker free.**

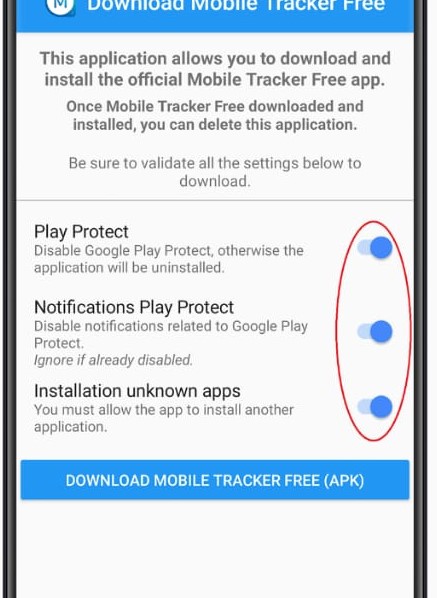
**8.Downloading the file.**

****

**9.Installing the apk file on victium phone.**

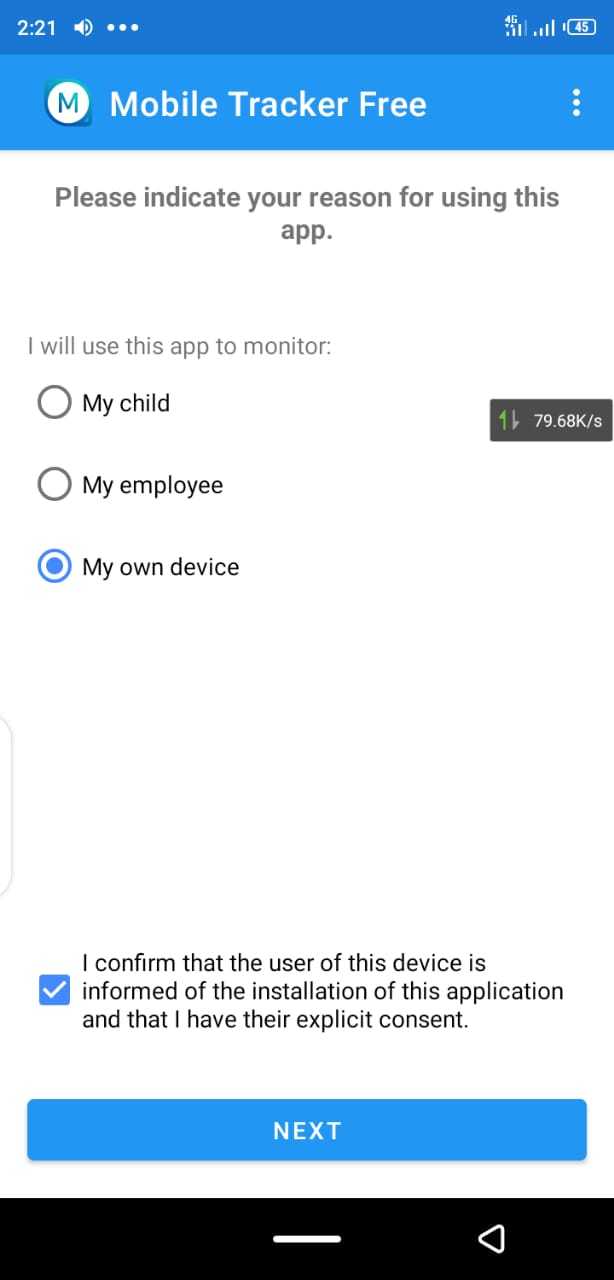
****

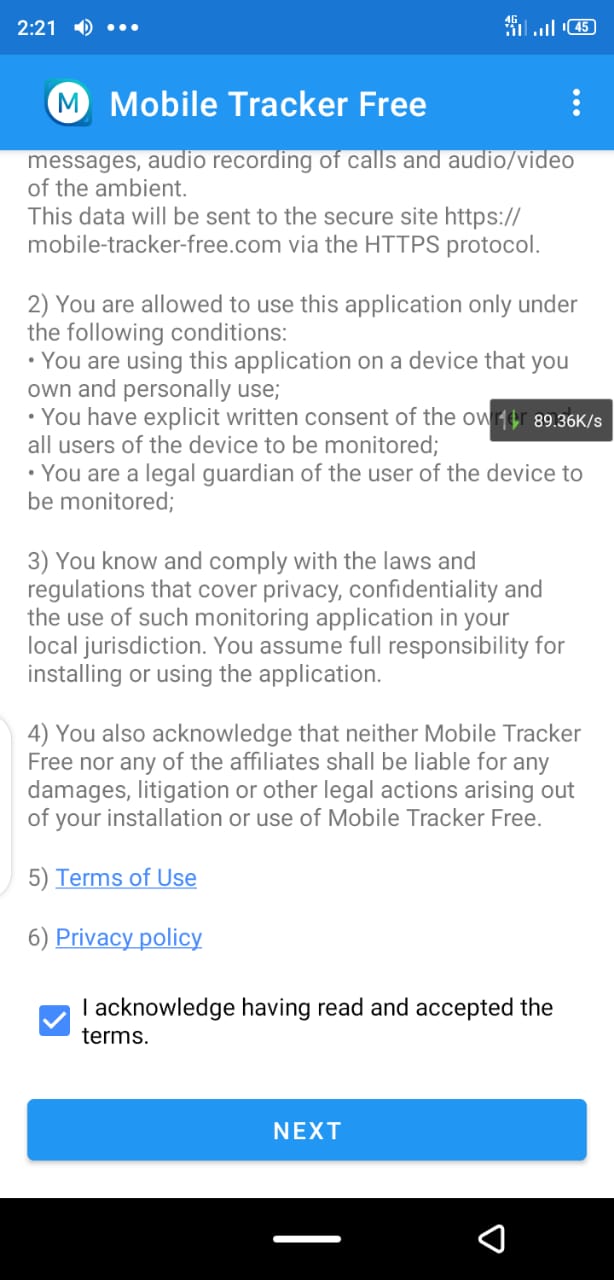
**10. Enable the all the permissions.click on download apk file.**

****

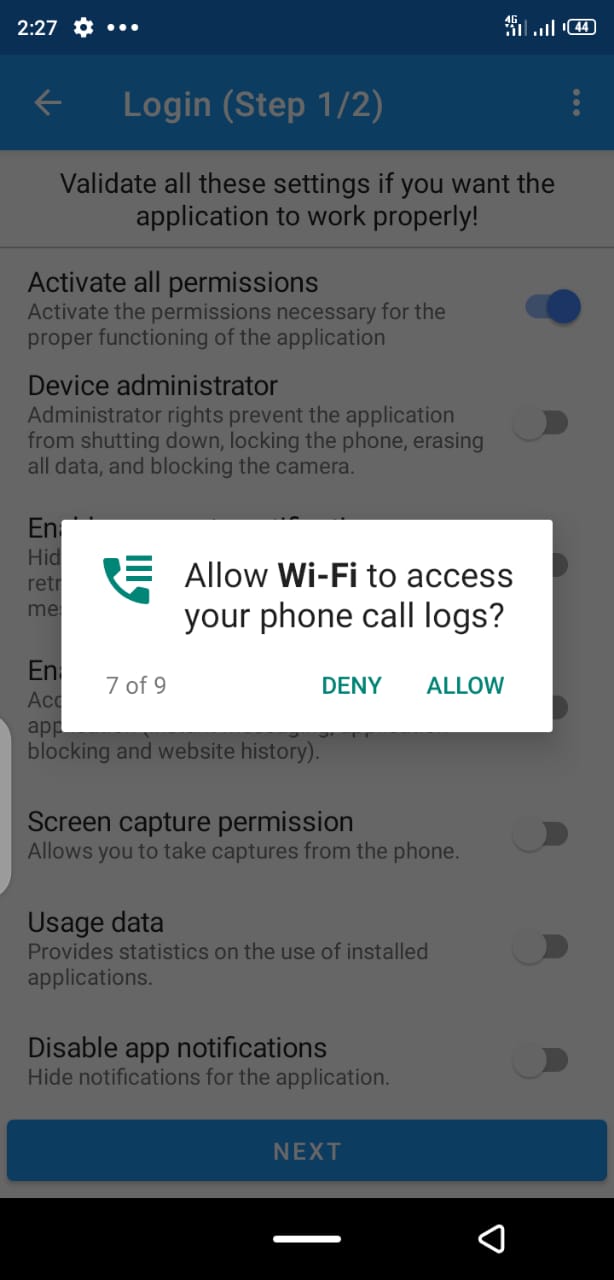
**11. we will install the wifi app.Open the app it will show like this.**

**Select the my own device And Click on next.**

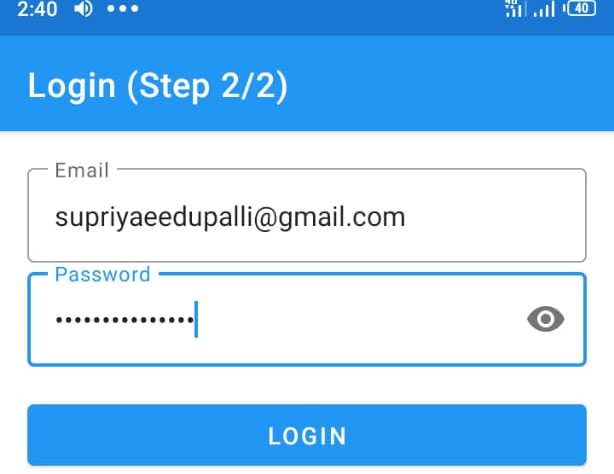
****

****

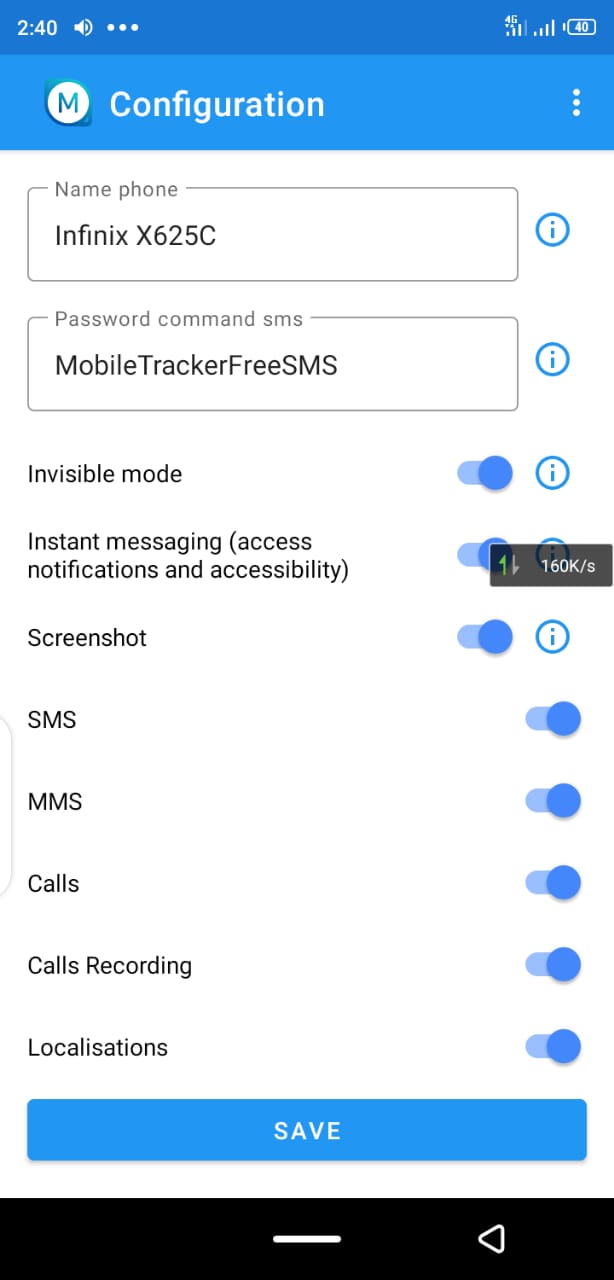
**12. Allow the all the permissions.**

****

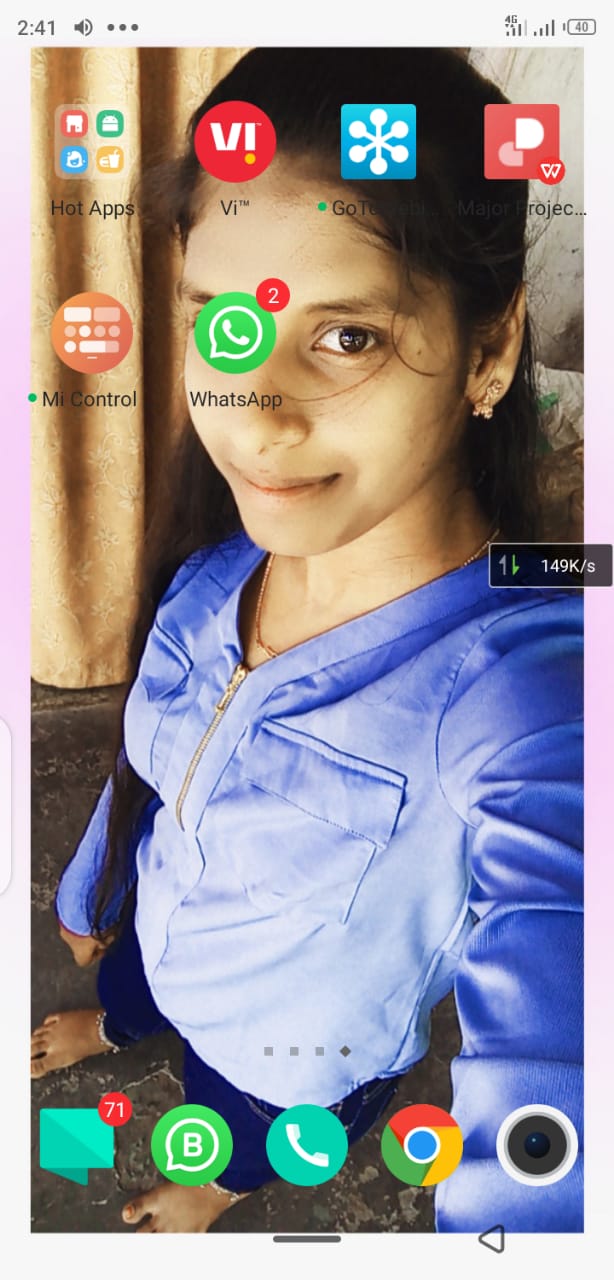
**13. Login the your id and password in “wifi app”.**

****

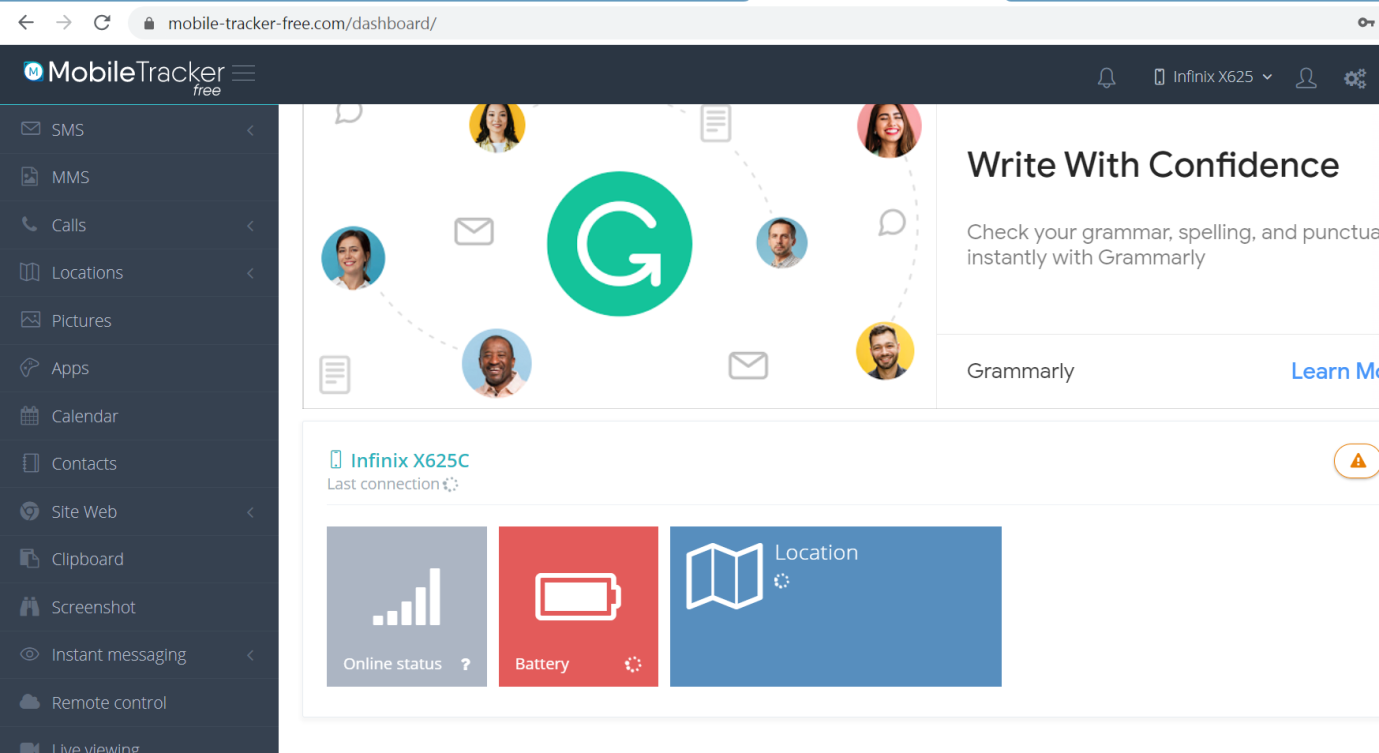
**14. Allow the all the permissions on the “wifi” app.And ‘save’ the permissions.**

****

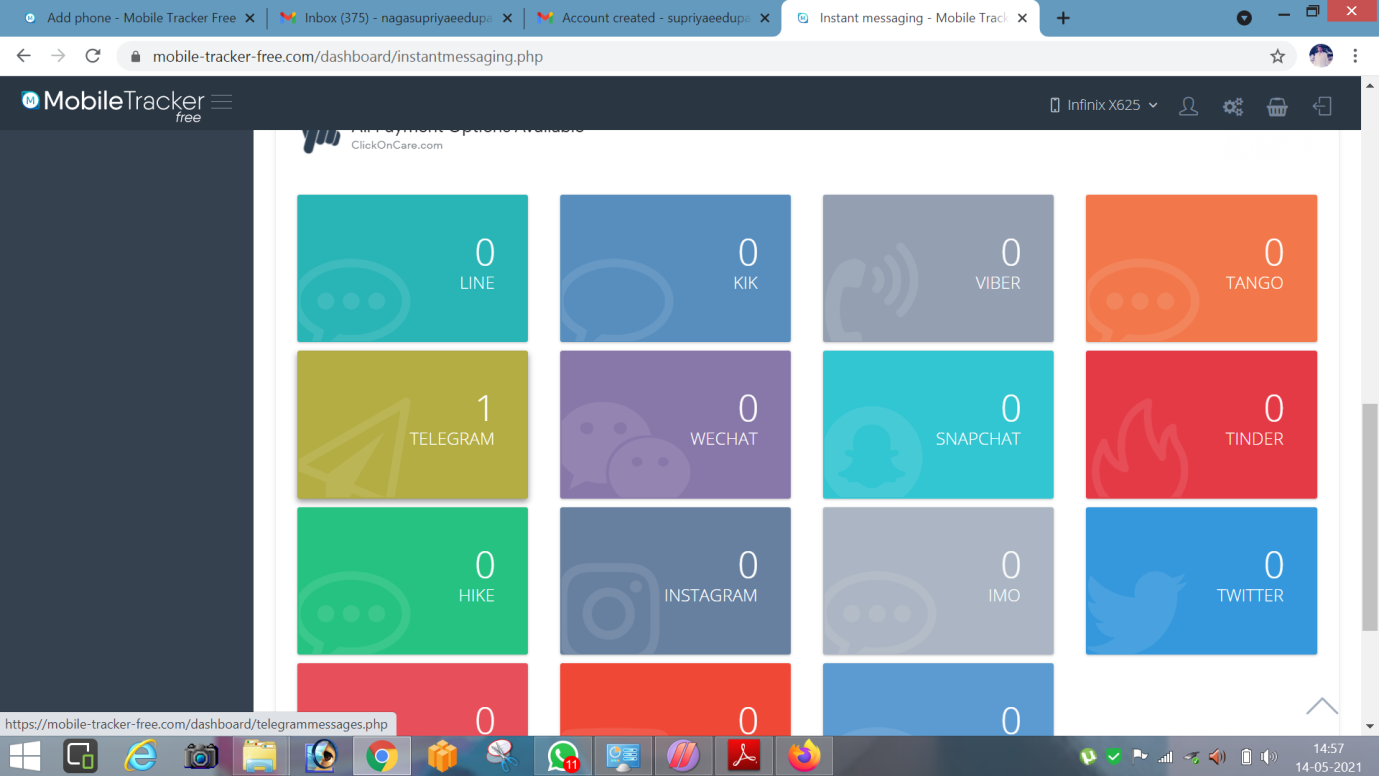
**15. After save the permissions the apps are hidden.**

****

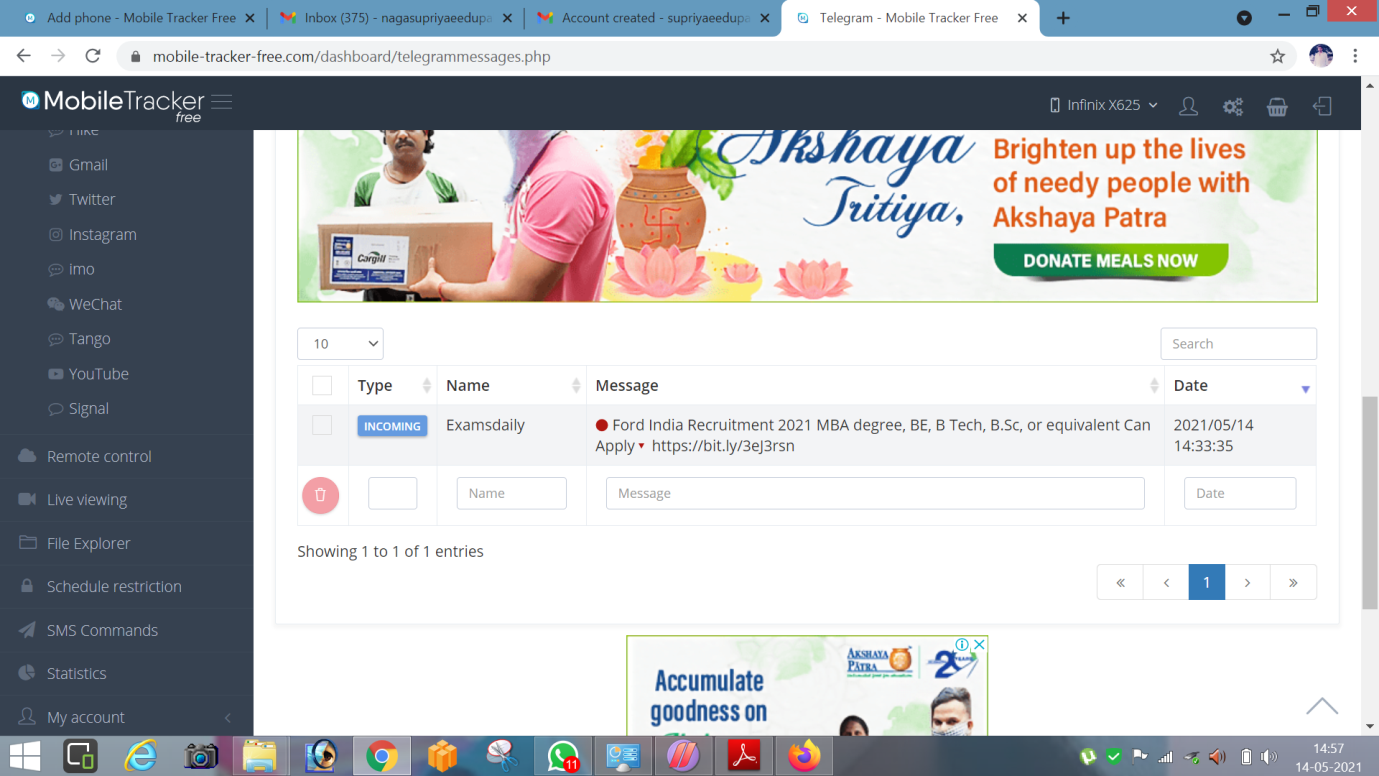
**16. Now ,Refresh on the your system mobile tracker login. My phone connected on the System.**

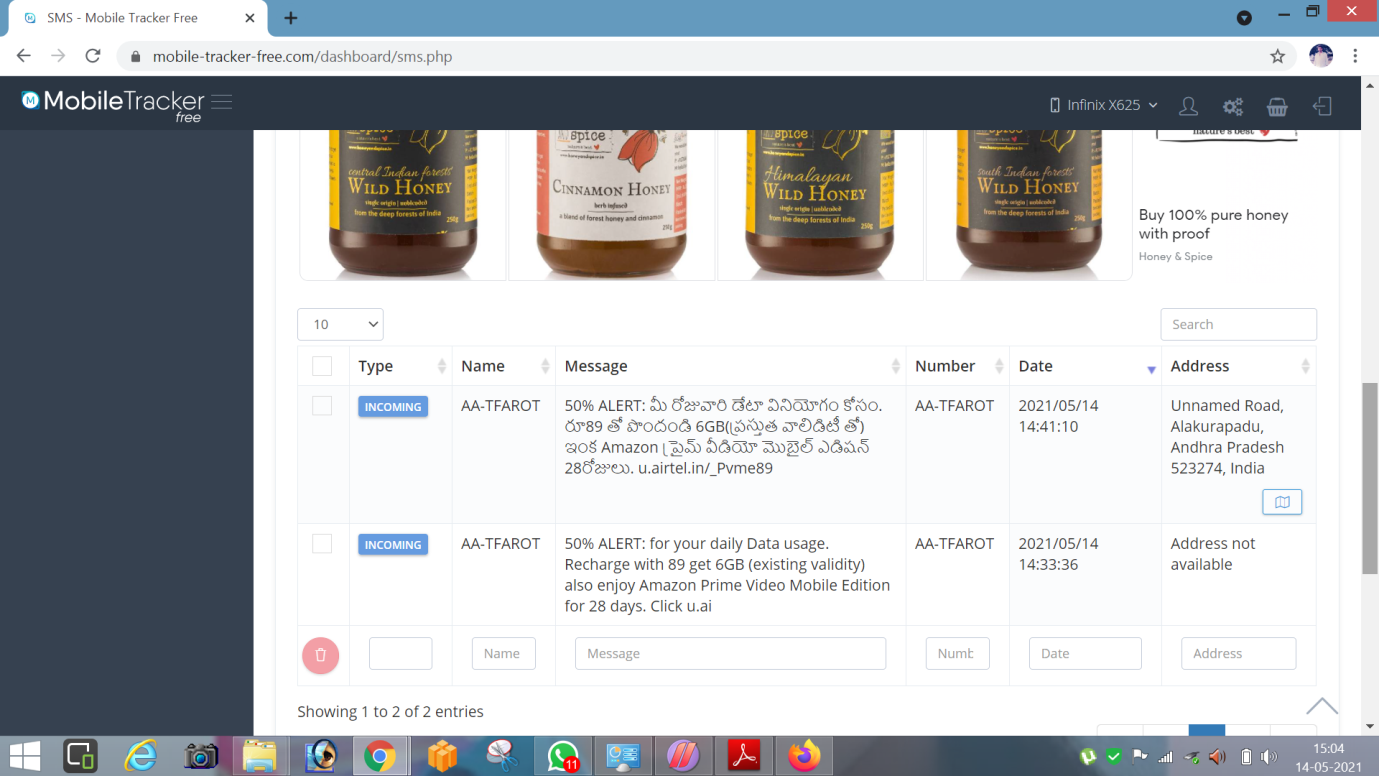
****

**17. We see on the WHATS APP OR TELEGRAM messages ,we go on the instance messages and click on the whatsapp or Telegram.**

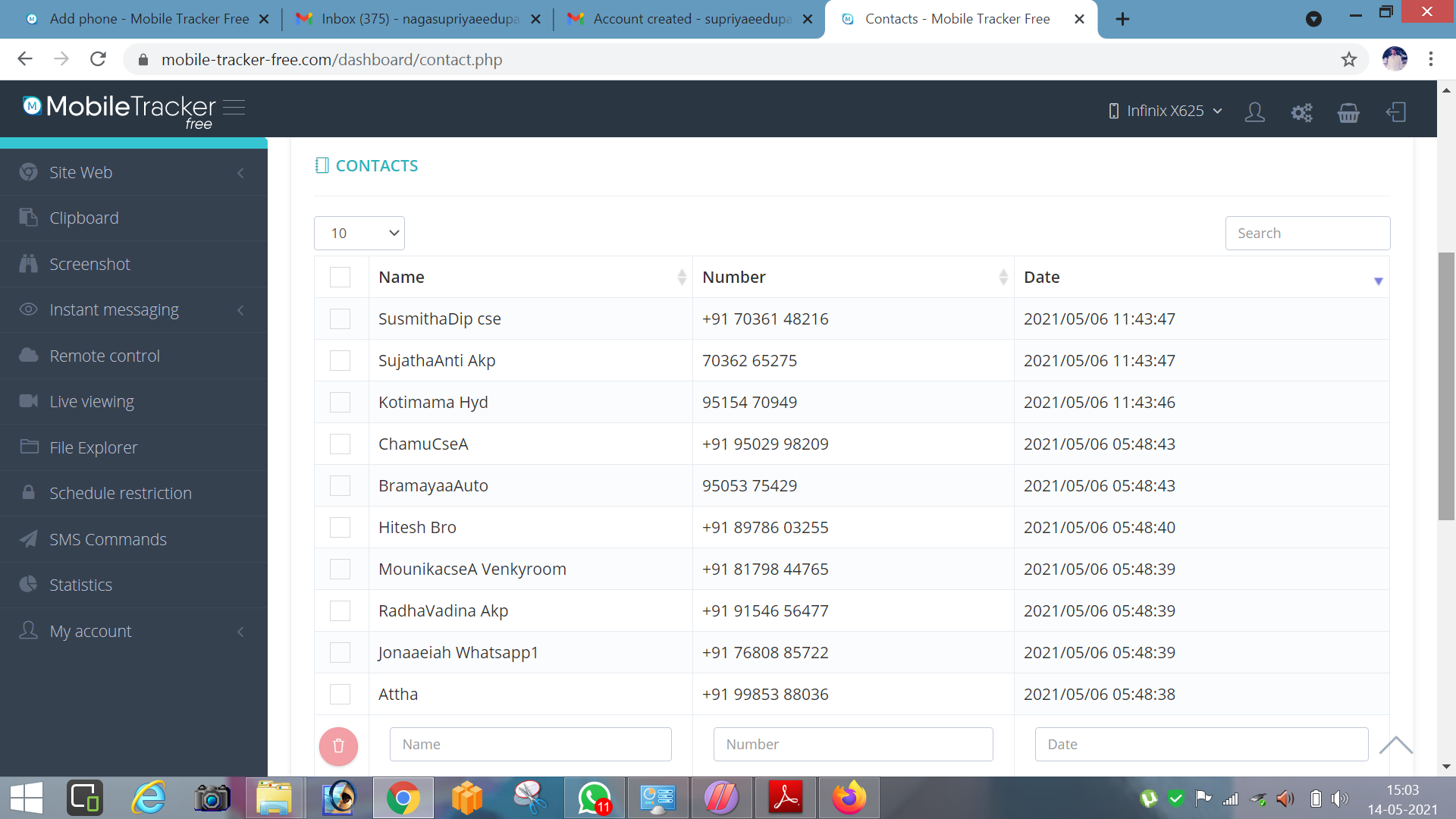
****

**18. Check the Telegram messages.**

****

**19.we see the Text messages also.**

**20. we see call history.**

****

**Solutions to avoid android hacking :**

If you’re still worried about hacking, there are further steps you can take to protect yourself. However, taking things too far will defeat the purpose of having a smartphone at all.

* **Avoid unsecured public WiFi.**:Hackers often target important locations such as bank accounts via public WiFi that can often be unsecured due to relaxed safety standards or even none at all.
* **Turn off your autocomplete feature.** By doing this, you can prevent stored critical personal data from being accessed.
* **Regularly delete your browsing history, cookies, and cache.** Removing your virtual footprint is important in minimizing the amount of data that can be harvested by prying eyes.
* **Have an iPhone? Enable Find My iPhone.** By turning the feature on in your settings, you’ll be able to locate your phone if you misplace it before the hackers can lay their paws on it.
* **Use a security app that increases protection.**For Android owners, Webroot offers the all-in-one [Mobile Security for Android app](https://www.webroot.com/us/en/home/products/antivirus-for-android) that provides antivirus protection and allows you to remotely locate, lock up and wipe your phone in the event you lose track of it. For iOS users, Webroot also offers a free secure web browser for [increased mobile security](https://www.webroot.com/us/en/home/products/ios-mobile-security) on your iPhone and iPad.
* **Never leave your phone unattended.**Keeping your phone with you at all times while in a public place is the first, best rule to follow.
* **Change your phone’s default passcode.** Your phone likely comes with a simple, predictable default password, and those who know can use this to their advantage. Change your code to something more complex, and resist the usual "1234," "0000" and “2580” codes that are commonly used.
* **Manage your Bluetooth Security.**Avoid using [unprotected Bluetooth networks](https://www.webroot.com/in/en/resources/tips-articles/a-review-of-bluetooth-attacks-and-how-to-secure-mobile-workforce-devices) and turn off your Bluetooth service when you aren’t using it.
* **Protect your PIN and Credit Card data.** Use a protected app to store PIN numbers and credit cards, or better yet, don’t store them in your phone at all.