# SECURE WAY OF USING SMART PHONE
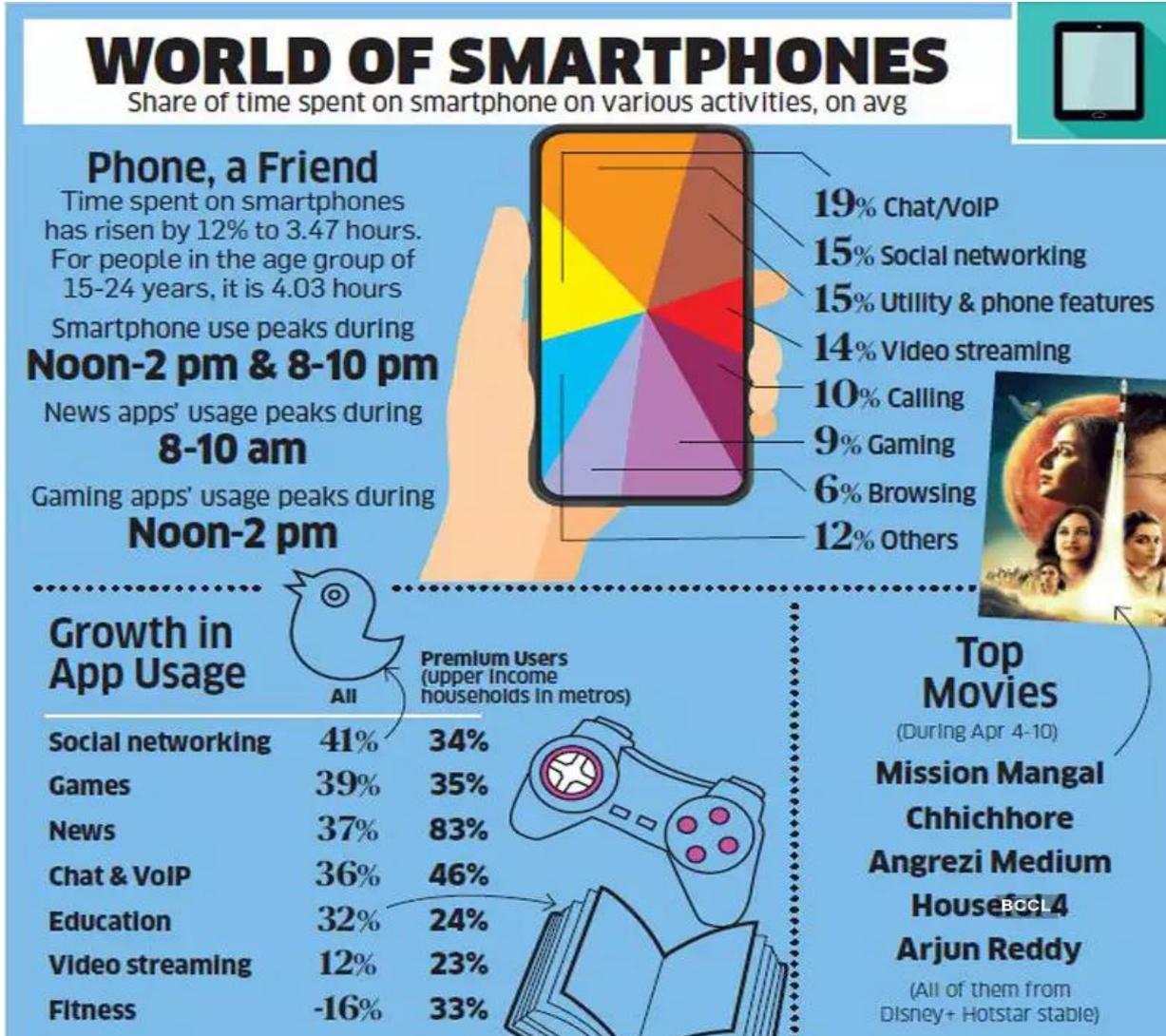
Indraveni K

Joint Director,

C-DAC, Hyderabad
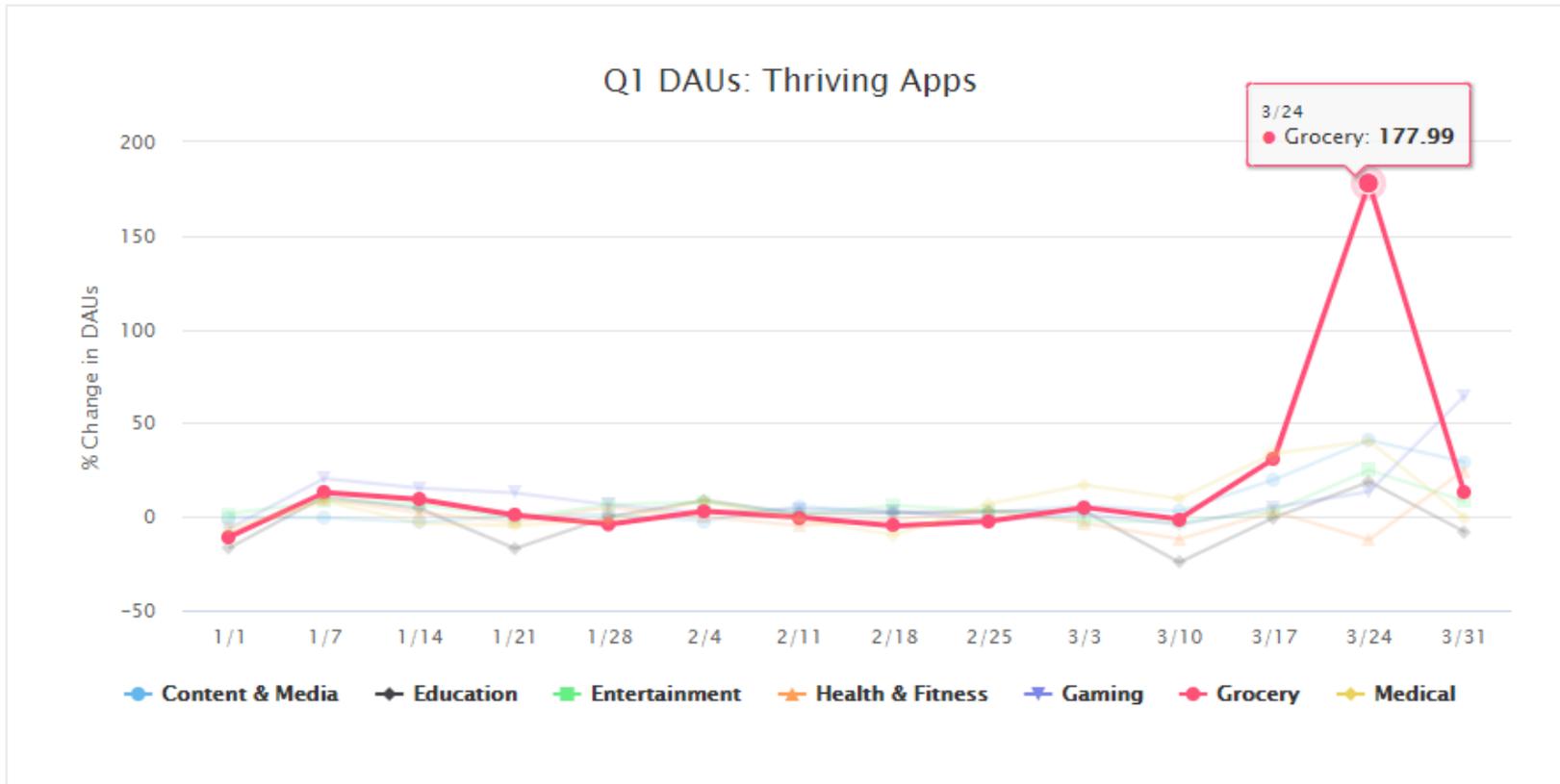
# Smart Phones usage

## WORLD OF SMARTPHONES
Share of time spent on smartphone on various activities, on avg

### Phone, a Friend
Time spent on smartphones has risen by 12% to 3.47 hours. For people in the age group of 15-24 years, it is 4.03 hours

Smartphone use peaks during
**Noon-2 pm & 8-10 pm**

News apps' usage peaks during
**8-10 am**

Gaming apps' usage peaks during
**Noon-2 pm**

- 19% Chat/VoIP
- 15% Social networking
- 15% Utility & phone features
- 14% Video streaming
- 10% Calling
- 9% Gaming
- 6% Browsing
- 12% Others

### Growth in App Usage

| | All | Premium Users (upper income households in metros) |
|---|---|---|
| Social networking | 41% | 34% |
| Games | 39% | 35% |
| News | 37% | 83% |
| Chat & VoIP | 36% | 46% |
| Education | 32% | 24% |
| Video streaming | 12% | 23% |
| Fitness | -16% | 33% |

### Top Movies
(During Apr 4-10)

**Mission Mangal**
**Chhichhore**
**Angrezi Medium**
**House 4**
BCCL
**Arjun Reddy**

(All of them from Disney+ Hotstar stable)

Economic Times

# Smart Phones usage

- Daily Active Users



CleverTap Q1 Data

# Why should we worry ?

- smartphones
  - Have our credentials are saved
  - Have our banking apps are installed
  - We carry out many financial transactions - upi, wallets etc.,
  - Messages
  - Photographs and videos

# Why should we worry ?

Our complete

Personal Sensitive

Information is carried by our smart phones

# Critical Features of your mobile

- Messaging – OTP , password research codes etc.,

- Camera

- Microphone

- Gallery

- Contacts

- Location

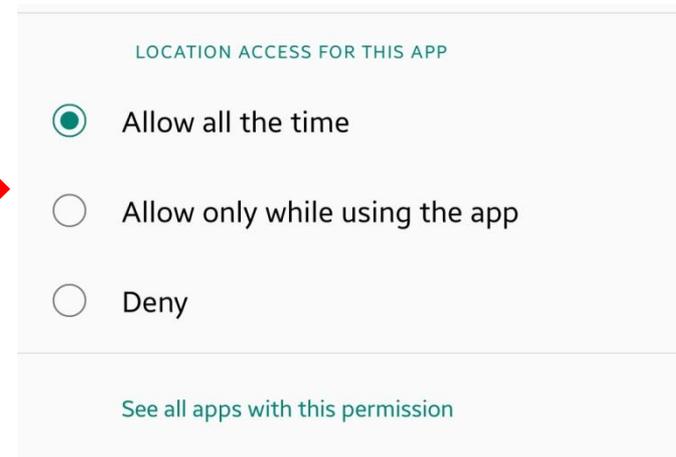**Regularly Monitor the permissions of critical features of your mobile**
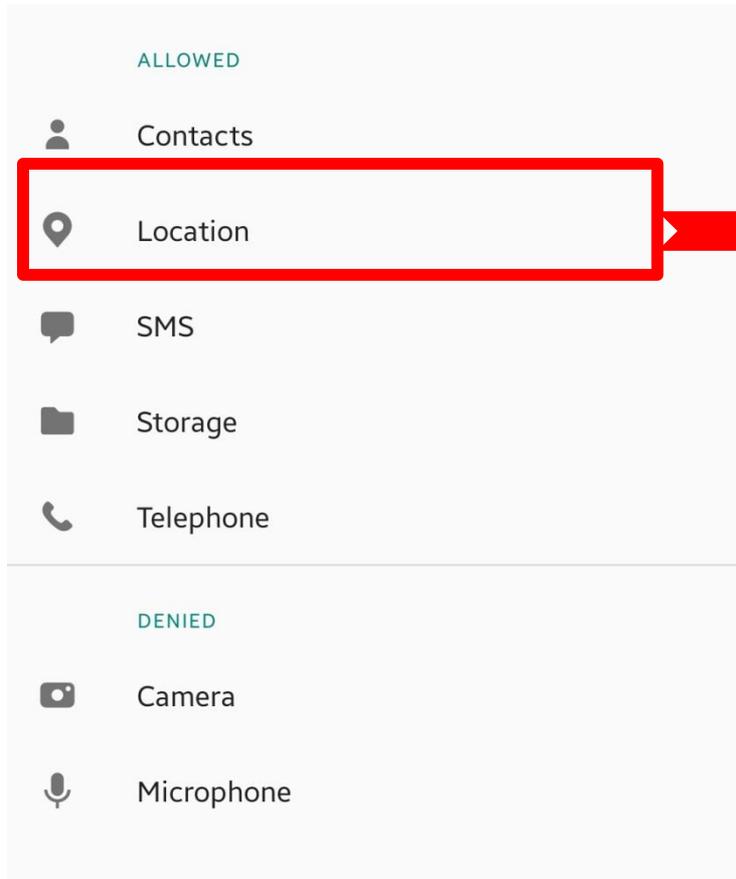
# Monitor Permissions

- Settings - Apps
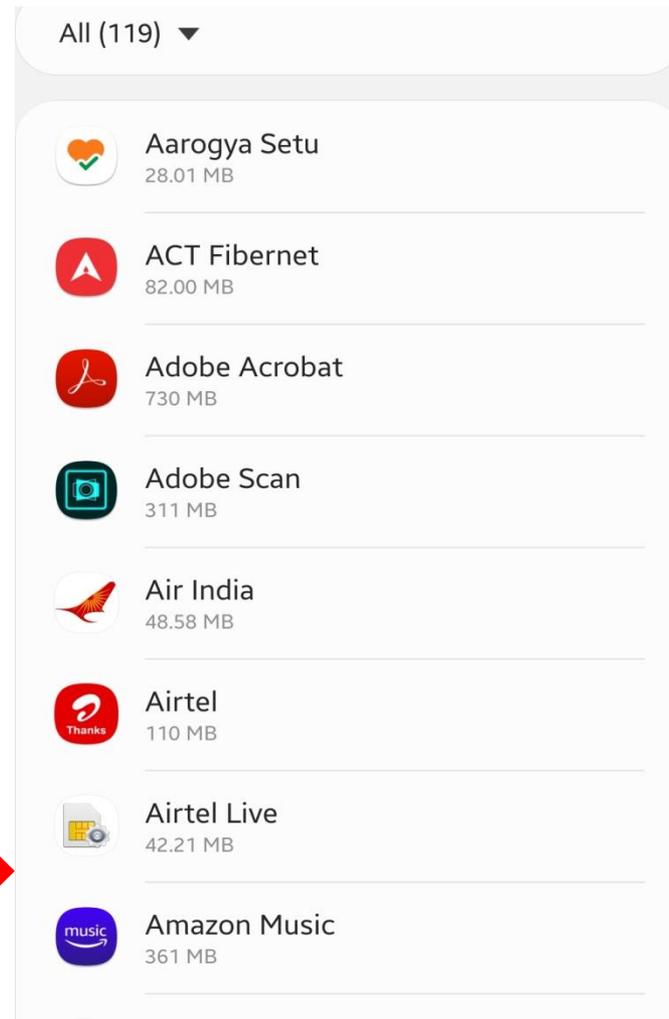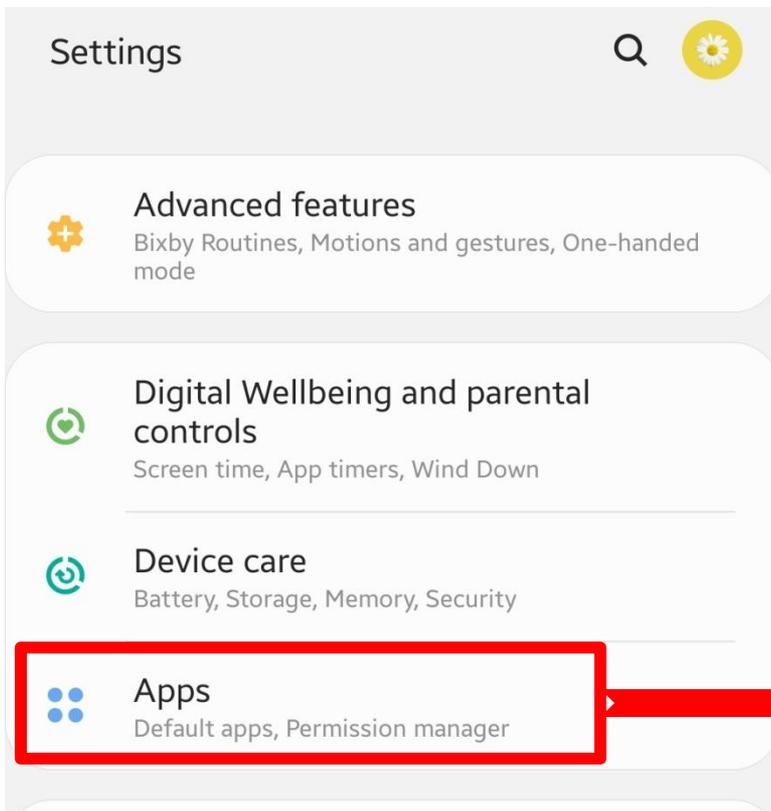
# Monitor Permissions
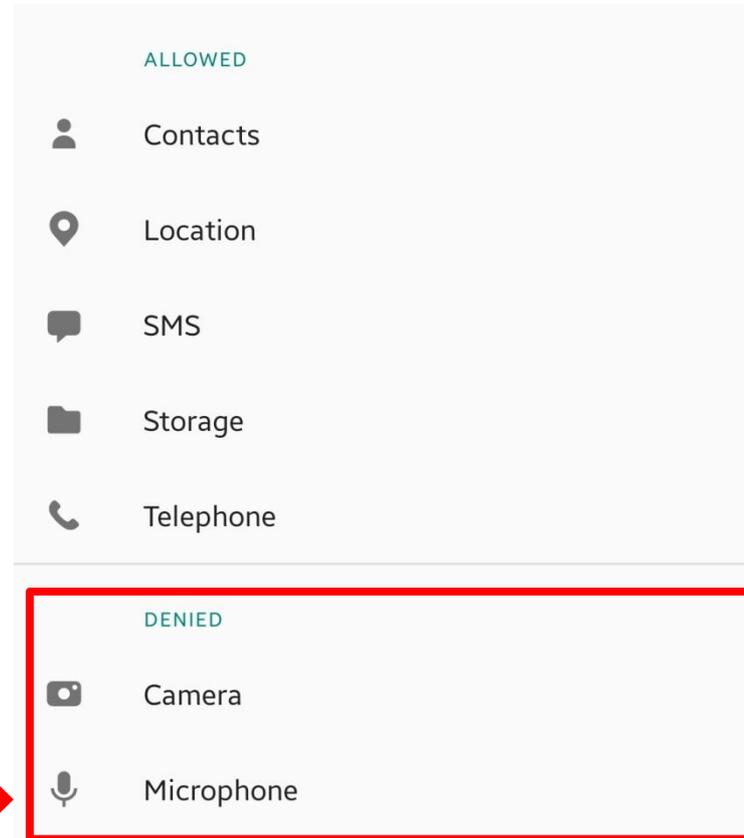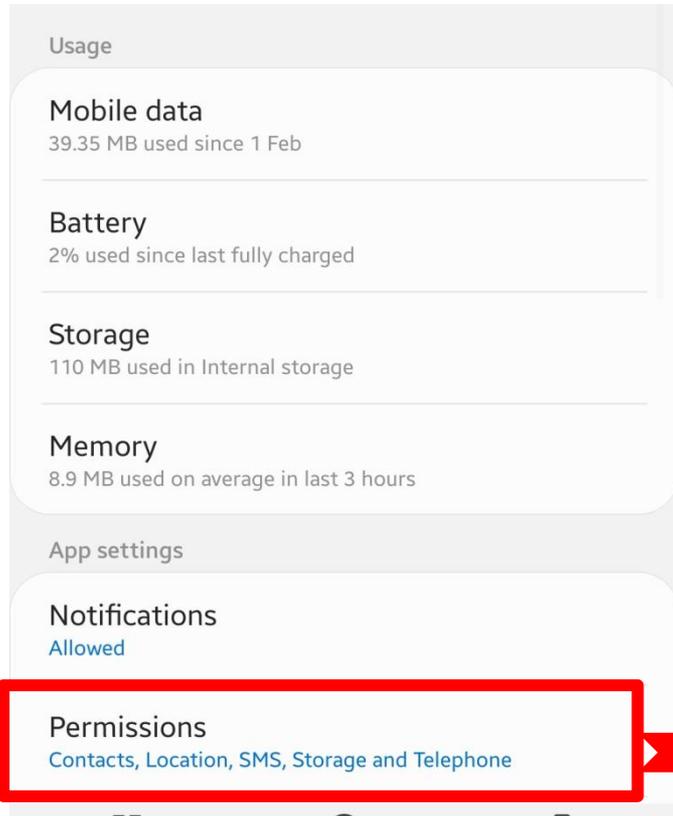


Based on App functionality we should be able to analyze
if these permissions are necessary for the app or not

# Change Permissions

**ALLOWED**

- Contacts
- Location
- SMS
- Storage
- Telephone

**DENIED**

- Camera
- Microphone

**LOCATION ACCESS FOR THIS APP**

- ⦿ Allow all the time
- ○ Allow only while using the app
- ○ Deny

See all apps with this permission
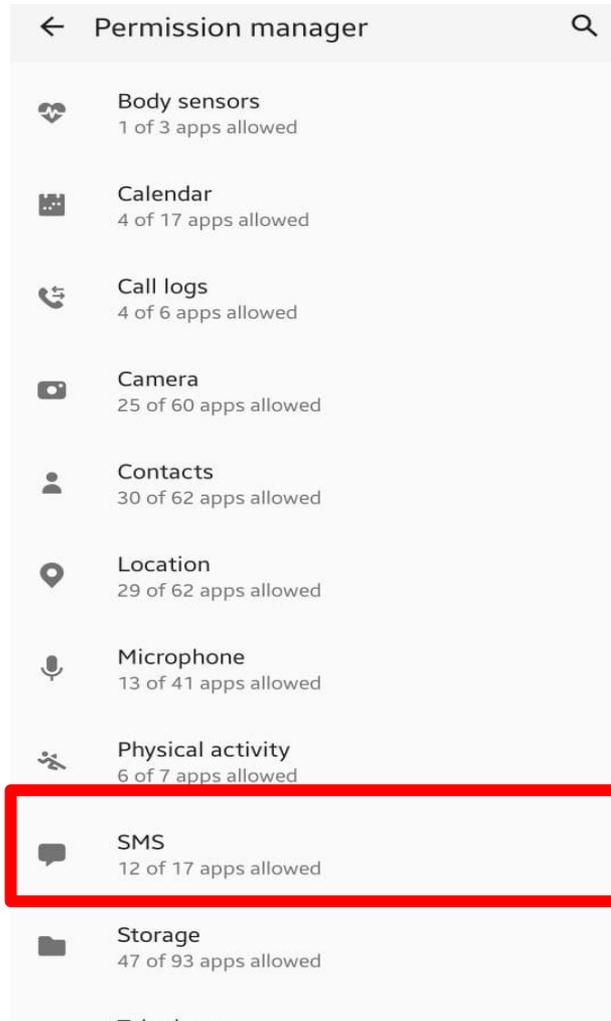
# Monitor all critical permissions at one place

- Access Permission Manager in your Mobile
  - Settings – Apps – Permission Manager (OR)
  - Settings - Privacy
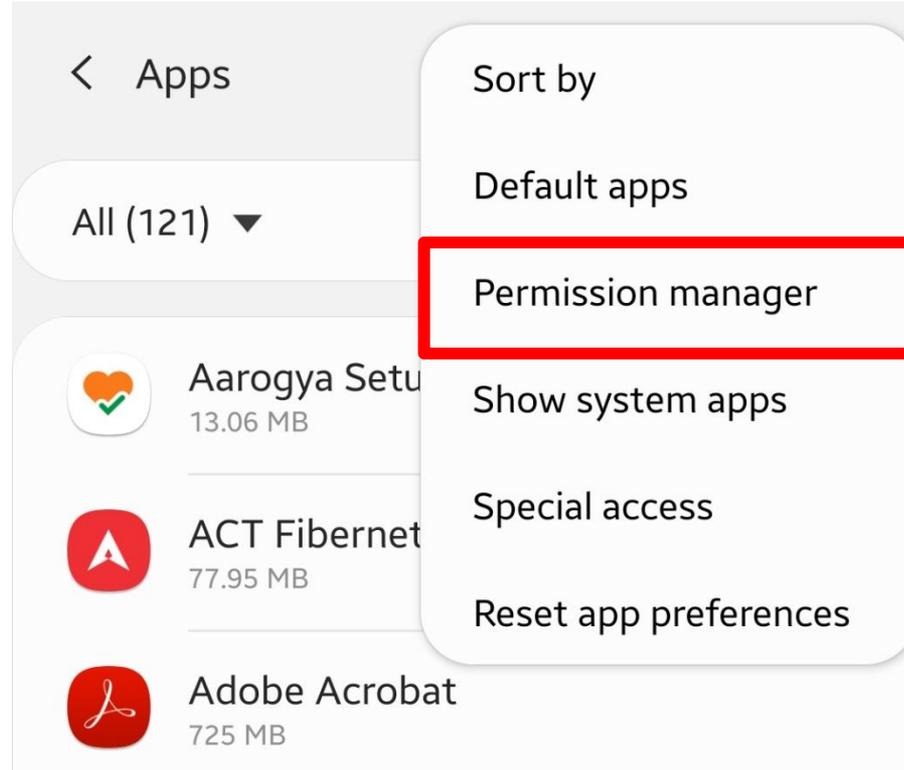
# Monitor all critical permissions at one place

- Permission Manager
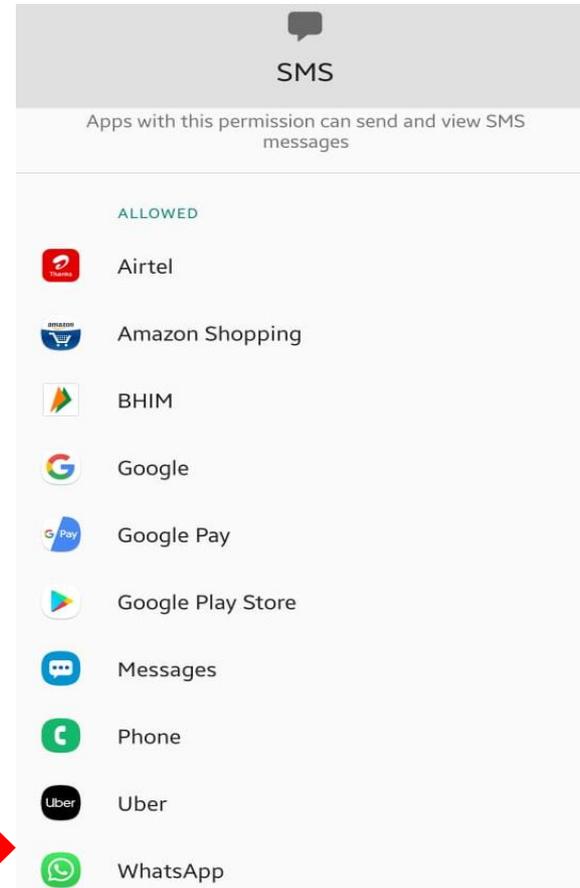
# Symptoms

- If OTP is filled automatically by your application while performing any transaction or filling any page, it means that the app is having permissions to read your SMS automatically.

- If in your browser without entering your credentials, you are able to see the logged in state of website, it means you browser saved your credentials

- Inspite of Turning OFF Location, Bluetooth , its automatically turned ON in some time, it means some app in controlling the same.

# Installing Apps

- Advertisements could be one of the medium to bring malware to your mobiles or steal personal information

- Sometimes, App download page itself states that it contains advertisements or you can see the reviews to know if it contains advertisements

- Reviews also can help understand Good and Bad about apps

**Avoid installing apps which contains advertisements and read reviews before installing**

# Installing Apps

- Search in stores can lead to malicious/phishing apps.

- For apps related to payment, banking , social networking etc., prefer to download app from company's owned website rather than searching in the stores.

# Example – search for PNB banking app

# Example – Link from Original Bank website

# Say No to All-In-One Apps

# Installing Apps

- Search in stores can lead to malicious/phishing apps.

- For apps related to payment, banking , social networking etc., prefer to download app from company's owned website rather than searching in the stores.

**Download apps from genuine link & avoid all in one apps for any requirement**

# Unused Apps

- Monitor your mobile for <span style="color:red">unused apps</span> – Look in play store by sorting with Last used to know which apps were not used by you since long time.
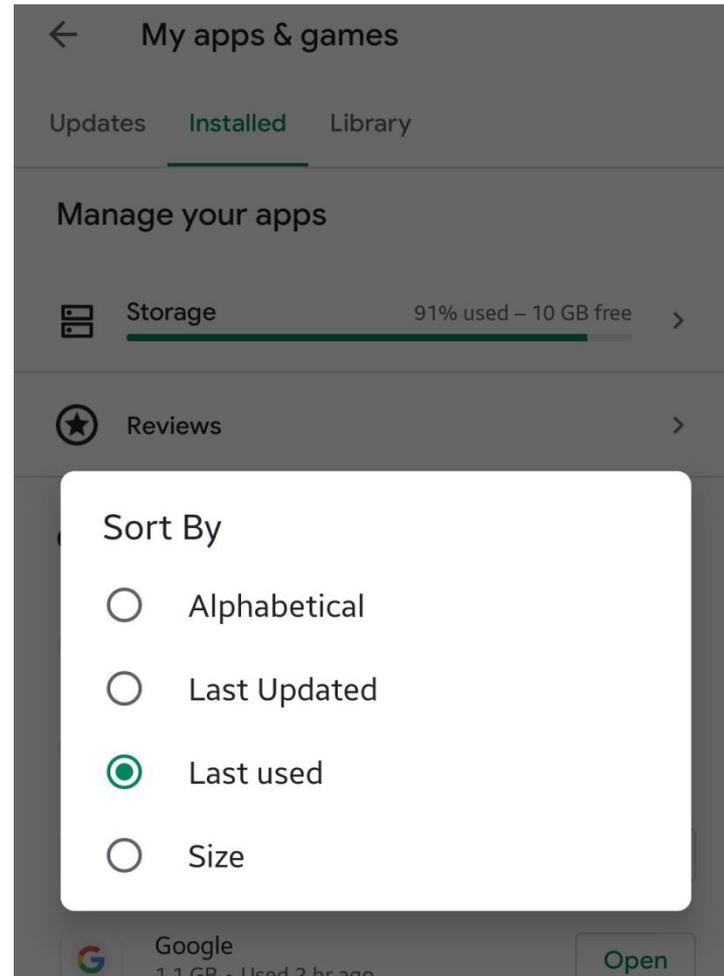
# Updated Operating System and Apps

- Ensure your anti-virus and operating system are always updated

- Settings -> Software Update

< Software update

Your software is up to date.

Software update information

- Current version: A507FNXXU3BTB2 / A507FNODM3BTB3 / A507FNXXU3BTB2
- Security patch level: 1 February 2020

**QUICK TIP**
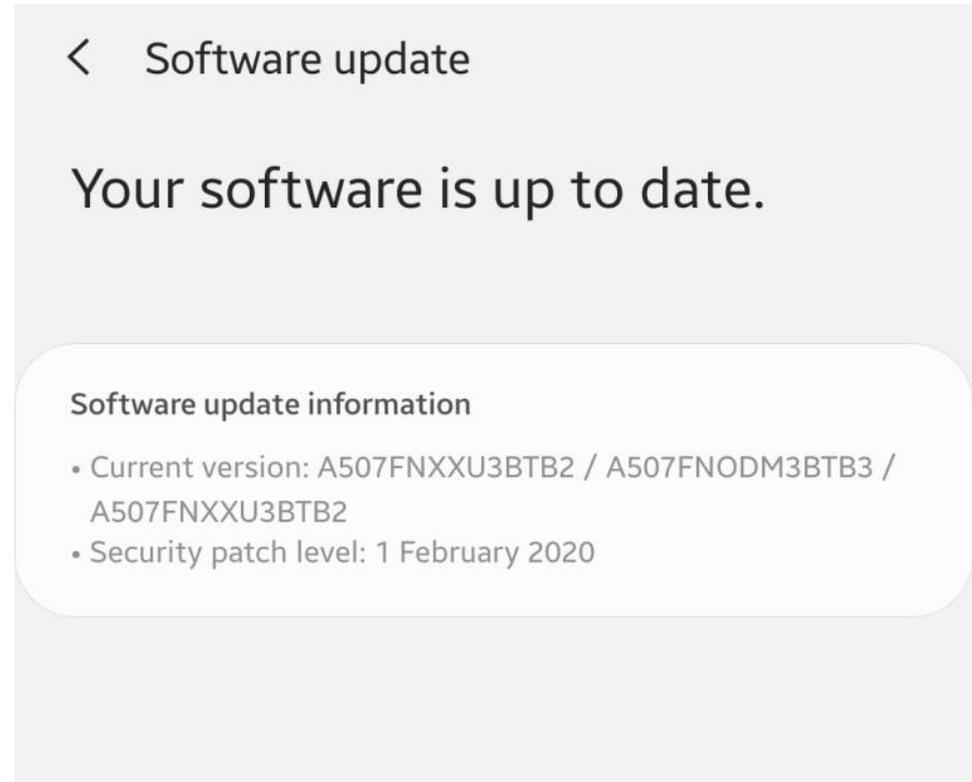
Ensure Auto Updates are enabled for OS, Apps and Anti-Virus

# WhatsApp Security – Tip 1

WhatsApp Settings - Account - Privacy

### Privacy

**Who can see my personal info**

If you don't share your Last Seen, you won't be able to see other people's Last Seen

**Last seen**
Nobody

**Profile photo**
My contacts
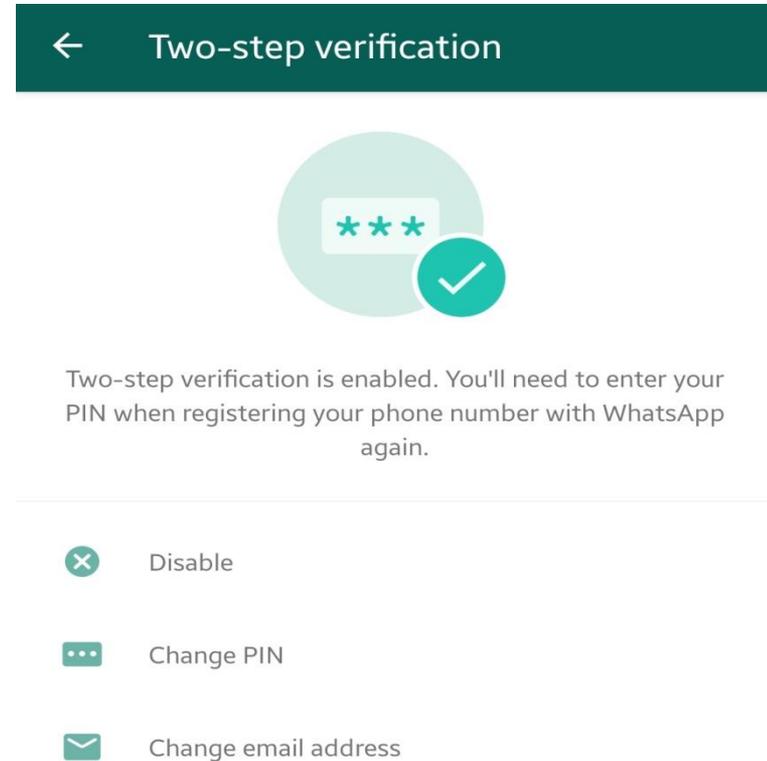
**About**
Nobody

**Status**
My contacts

**QUICK TIP**

**Control Visibility of your Profile Photo and Status to limited or contacts only**

# WhatsApp Security - Tip 2

WhatsApp Settings -
Account – Two –
factor
Authentication

**Two-step verification**

Two-step verification is enabled. You'll need to enter your PIN when registering your phone number with WhatsApp again.

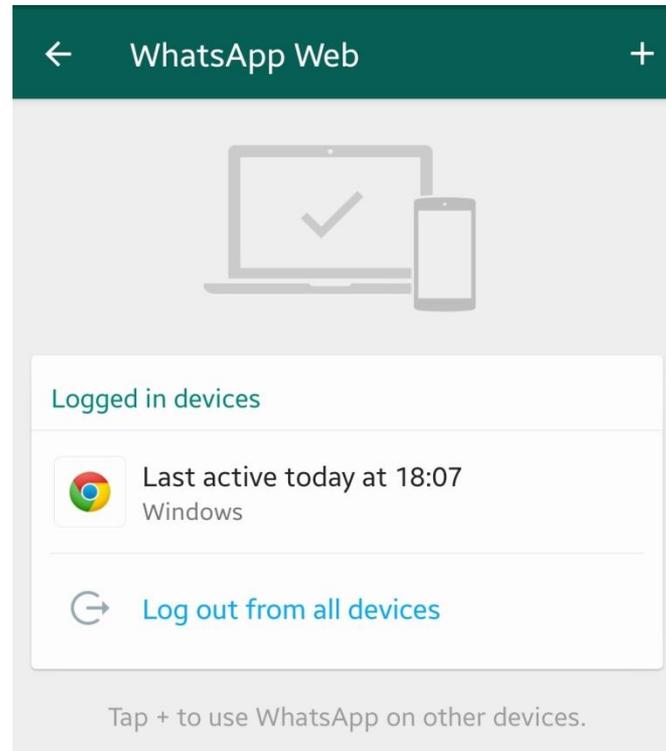Disable

Change PIN

Change email address

QUICK TIP

**Enable two-factor authentication to stop unauthorized registration of your whatsapp account**

# WhatsApp Security  - Tip  3

WhatsApp Settings
– WhatsApp Web



**QUICK TIP**

**Logout Web WhatsApp when not in use by you**
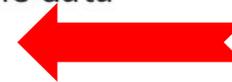
# WhatsApp Security  - Tip  4

WhatsApp Settings – Data and Storage usage

Media auto-download

Voice messages are always auto-downloaded for the best communication experience

When using mobile data
No media

When connected on Wi-Fi
No media

**QUICK TIP**

**Disable Auto-Download of Media**

# Safe Mobile Usage - Recap

1. Regularly Monitor the permissions of critical features of your mobile

2. Avoid installing apps which contains advertisements and read reviews before installing

3. Download apps from genuine link & avoid all in one apps for any requirement

4. Ensure Auto Updates are enabled for OS, Apps and Anti-Virus

5. Whatsapp Security
    1. Control Visibility of your Profile Photo and Status to limited or contacts only
    2. Enable two-factor authentication to stop unauthorized registration of your whatsapp account
    3. Logout Web WhatsApp when not in use by you
    4. Disable Auto-Download of Media

# Tips for your daily practice

- Turn OFF Bluetooth and Wifi when not in use
- Set time limit and Lock mobile automatically when not in use
- Prefer PIN/ finger print / face recognition locks as supported by your mobile.
  - Pattern lock are to be avoided -  beware of shoulder surfing , screen reading by placing mobile in different positions.
- Track your mobile for unnecessary and unused apps

# THANKYOU

Visit www.infosecawareness.in for more details