Safe Practices While Using Mobile Phones

By
M K Chaithanya
C-DAC Hyderabad

Outline

- Introduction
- Statistics of Mobile Usage
- Current State of Mobile Security
- Recent Attacks
- Various Mobile Threats
- Privacy Configurations
- Security Tips

Introduction

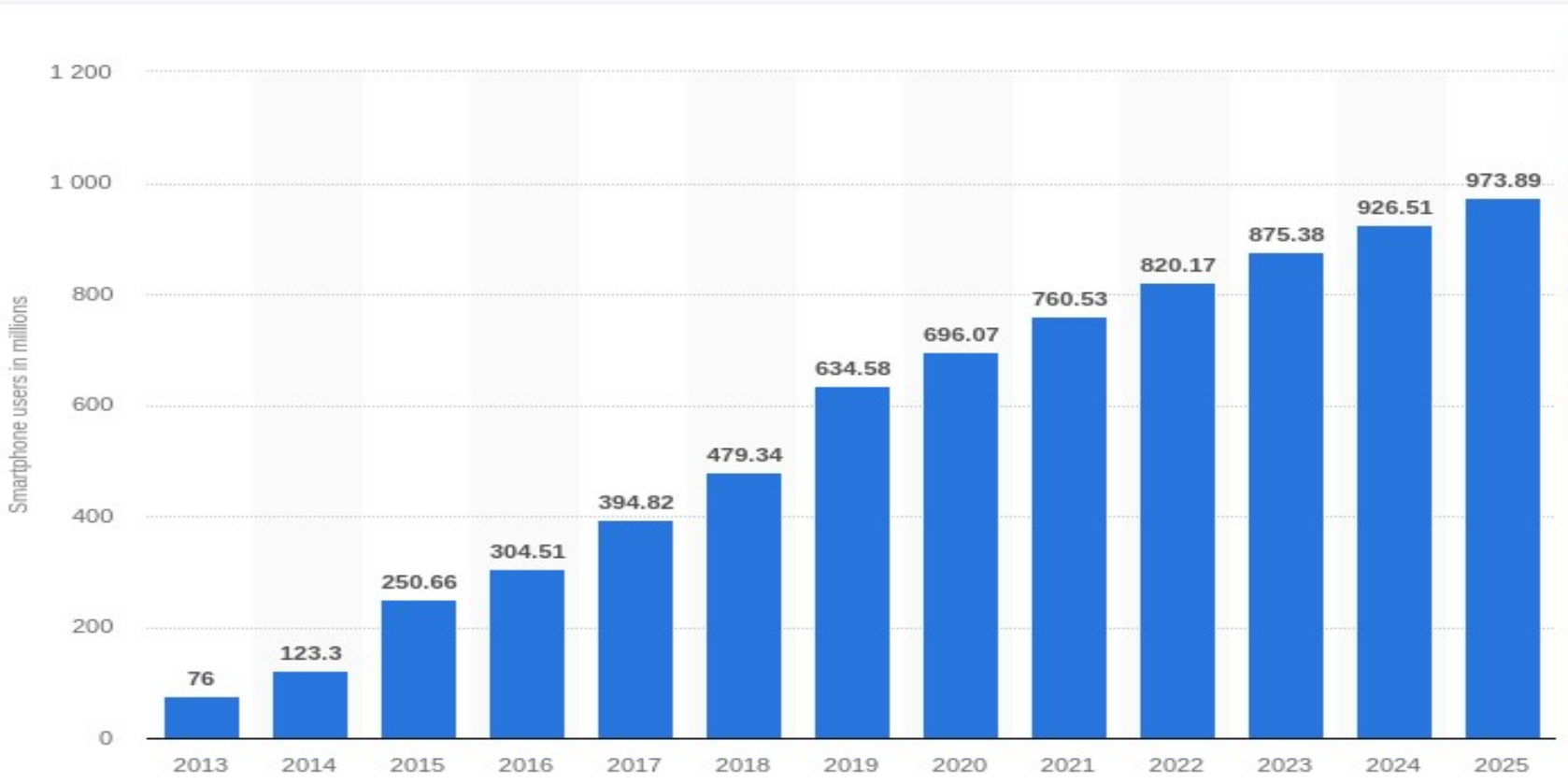
- Mobile devices have revolutionized the way we
  - Communicate
  - Surf the internet
  - Do payments and many more
- They have the capability to perform the functionality of a
  - Camera
  - Scanner
  - Audio recorder and many more

Introduction

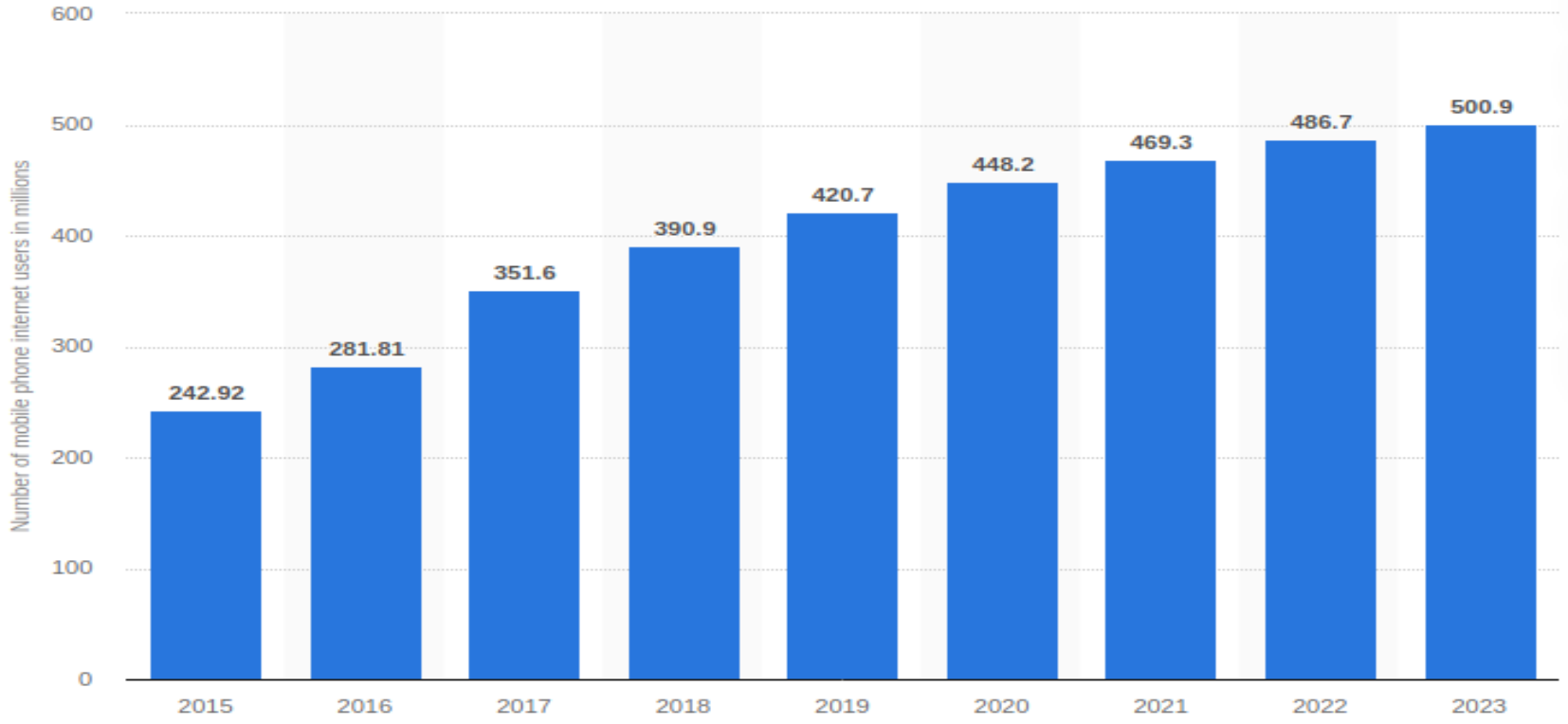
- This multi function capability has made mobile devices an important part of personal and business life
- This has led to tremendous increase in the usage of mobile devices in the country

Current State of Mobile Device Usage in the Country

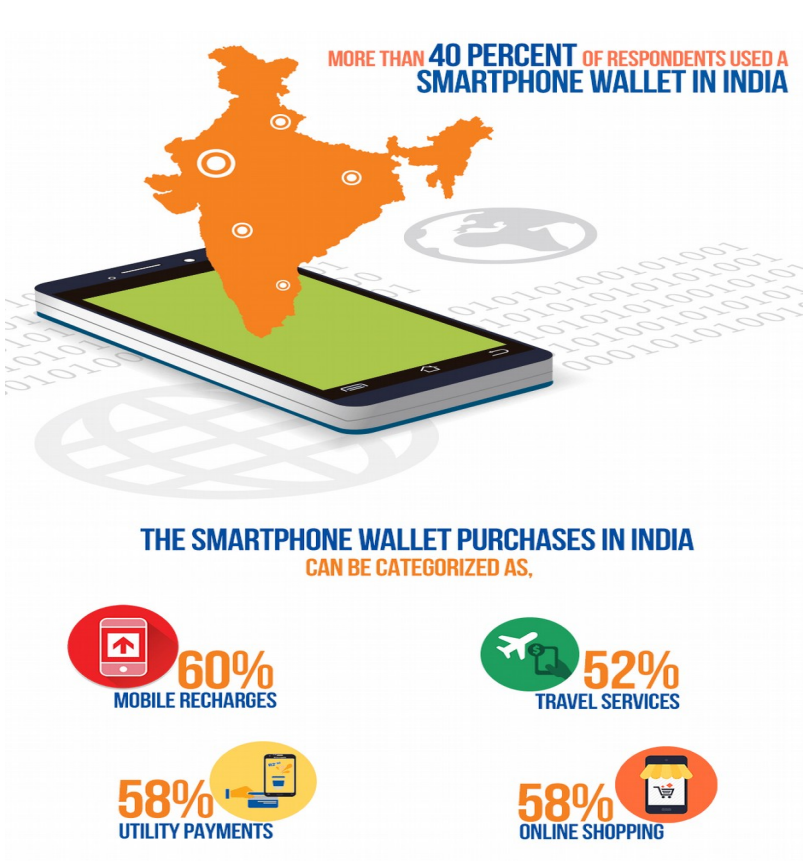
Smart Phone users in India



Mobile Internet Users in India



Mobile Payments in India



Major cause for increase in mobile threats

- This tremendous increase in the usage of mobile devices has led to huge amounts of personal and business related data being stored and accessed on the mobile devices
- This same reason has become the motivation for hackers and attackers to target these devices which have become mini hubs of rich data

Popularity of Android platform

Current State of Mobile Security in the Country

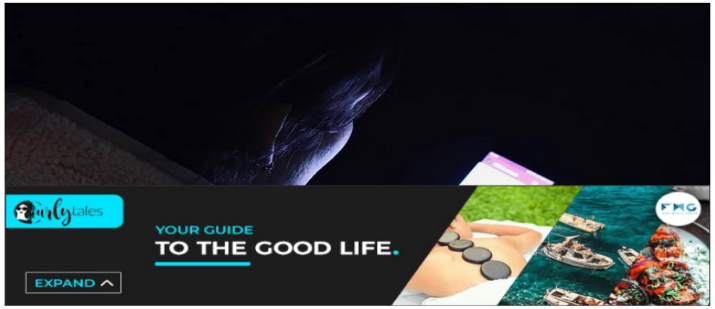
Smartphones became hotspots of cyber attacks in India

- If you are thinking that only large critical infrastructure and big corporations would be targeted for cyber attacks, you are wrong
- In India, smartphones, the device that most people now carry in their pockets, have become a very large attack centre, said a top security expert at Check Point

Mobile malware attacks continue to rise in India since October 2020: Check Point

The latest 2021 Mobile Security report by Check Point asserts that there were around 1,345 mobile attacks in October 2020 and a whopping 12,719 attacks were reported in March 2021.

By: **Tech Desk** | New Delhi |
Updated: April 14, 2021 1:20:40 pm



Over 845% increase seen in mobile attacks since October 2020: Report (Photo: Pixabay)

India has witnessed over 845 per cent increase in mobile attacks since October 2020 with people continuing working from home due to COVID-19 pandemic. The latest 2021 Mobile Security report by Check Point asserts that there were around 1,345 mobile attacks in October 2020, which jumped to 12,719 attacks in March 2021.

MORE TECH


Technology
WWDC 2021: What to expect from Apple's iOS 15


Technology
Computex 2021: All announcements from AMD, Nvidia and Intel


Technology
Xiaomi Mi 11 Ultra delayed indefinitely;

Some Facts

- Bulk of the mobile phones in India are running a very old version of Android
- Mobile hardware is not manufactured in the country nor is the software that runs on it
- Even the anti-malware solutions being used in the country are neither designed nor developed in the country

Some Facts

- There are numerous fake banking applications and wallets detected in the Google playstore targeting victims in India which mimic the names or graphic design specifications of existing apps
- Insecure mobile browsers are posing a serious threat to the security and privacy of mobile users in the country
- Anti-Virus companies are extracting lot of analytical information from the users

Some Mobile Security Statistics 2021

- Four out of every 10 mobile phones are inherently vulnerable to cyber-attacks
- 97% of organisations globally in 2020 faced mobile threats 46% had at least one employee download a malicious mobile app
- With work from home becoming the new norm, attacks on personal handsets used for office work have been on a rise

Some Mobile Security Statistics 2021

- 93 percent of the attacks attempts to trick users into installing a malicious payload via infected websites or URLs
- Bogus COVID-19 related information apps have been used as a new target to hide malware, Check Point found.

Some Recent Attacks

Fake CoronaVirus Tracker App

- Hackers are misusing COVID-19 global pandemic to prey on naive users to steal financial credentials
- They have developed a malicious software named Coronavirus tracking Android app
- The COVID19 Tracker app is available for download on the website
- If any user comes to the site, he/she will be asked to download the Android app for the map

Contd..

- It says to offer the information on the spread of the pandemic in addition to country-wise statistics of COVID-19 infections, recoveries and fatalities
- Once installed, the Coronavirus app, which houses ransomware 'CovidLock' takes full control of the phone and blocks the user from opening the screen lock
- It demands a ransom of $100 in bitcoins to the victims
- Warns of permanently delete all the contacts, videos, images, messages and other personal information

Whats App Zero-Click Spyware Attack

- A vulnerability had been discovered that let attackers install spyware on iPhones and Android phones simply by placing a WhatsApp voice call to the user’s smartphone
- What’s notable about the WhatsApp attack is that it was a “zero-click” or “no click” attack.
- That means the spyware was able to be installed on a smartphone by the attacker simply placing a WhatsApp voice call to the phone.

Whats App Zero-Click Spyware Attack

- It does not matter if the call was answered or not–a target did not have to open any message, answer the call, or click on any link
- The spyware was allegedly created by the Israeli cyber surveillance company NSO Group.
- The secretive group creates spyware it sells to governments and law enforcement agencies around the world that allows them to take almost complete control of a device

Facebook's Data Deals

- Facebook's data deals are under criminal investigation
- For years, Facebook gave some of the world's largest technology companies more intrusive access to users' personal data than it has disclosed
- This emphasizes how personal data has become the most prized commodity of the digital age, traded on a vast scale by some of the most powerful companies

Contd..

- Facebook allowed Microsoft's Bing search engine to see the names of virtually all Facebook users' friends without consent
- The records show, and gave Netflix and Spotify the ability to read Facebook users' private messages
- The social network permitted Amazon to obtain users' names and contact information
- A political consulting firm, Cambridge Analytica, improperly used Facebook data to build tools that aided President Trump's 2016 campaign in US

Uber mishandles user's and driver's data

- San Francisco-based firm failed to closely monitor employees who had access to consumer and driver data
- It failed to deploy "reasonable measures" to secure personal information it stored on a third-party cloud provider's servers
- Uber is also being sued by a former employee who claims he was fired after blowing the whistle about insecure data practices at the company

Major Threats

- Hidden Apps
- Mobile Phishing
- Fake Mobile Apps
- Malware
- Spyware
- Adware
- Ransomware
- IoT Threats
- WiFi-Threats
- Data leaks
- Misconfiguration of devices

Fake Apps

- Fake mobile applications are applications that mimic the look and/or functionality of legitimate applications to trick unsuspecting users to install them
- Primary motto of Fakeapps include
  - Stealing of
    - Credentials
    - Financial Data
    - Business Data
    - Other Sesitive Data
  - Display of ads for revenue

How fake applications are built

- Built for a popular brand that doesn’t have an application of its own
- Cloning of existing applications and adding malicious code by tampering and repackaging

Distribution of fake applications

- Hosted on third-party app stores
- Circulated through social engineering campaigns
- Official app stores such as Google Play stores
- emails and SMS messages that appear to be from bank, credit card company or other brands
- As a notification for security updates

Few parameters that help in detection

- Number of app downloads
- App reviews
- Developer of the application
  - The more apps that developer has created, the higher the chance that the developer is real
- Visual things such as spelling errors, logos of poor quality and unbalanced or poorly formatted interfaces are clues that the app may be fake

Some recent fake apps detected

- Hackers stealing money via 167 fake Android - 17th May 2021
  - Majority of apps found are very similar
  - Attackers targeted users through dataing sites and lured victims into installing money stealing apps
  - Some apps even contain a customer support “Chat” option
  - These fake applications impersonate popular and trusted financial apps
  - All the applications are from the same group

Source: https://m.dailyhunt.in/news/india/english/indiatvnews-epaper-intvnews/hackers+stealing+money+via+167+fake+android+ios+apps-newsid-n280379606?s=a&uu=0xd074ffd0eb24ab9f&ss=wsp

Some recent fake apps detected

- 28 Fake Apps removed from Google Play Store post Quick Heal Security Lab reports
- These apps do not have any legitimate functionality related to App name
  - Credit card process
    - description on play store is “provide credit card process” but in the actual application there is no information related to the credit card process
  - Home Loan Advisor
    - description on play store is, “Gives advice for home loan” but in the actual application there isn’t any information related to home loan advice
- All apps are found to be developed by same developer

Mobile Phishing

- **If You Can Raed Tihs, You Msut Be Raelly Smrat**
- *"Aoccdrnig to a rscheearch at Cmabrigde Uinervtisy, it deosn't mttaer in waht oredr the ltteers in a wrod are, the olny iprmoatnt tihng is taht the frist and lsat ltteers be at the rghit pclae. The rset can be a toatl mses and you can sitll raed it wouthit porbelm. Tihs is bcuseae the huamn mnid deos not raed ervey lteter by istlef, but the wrod as a wlohe."*

Contd..

- Phishing attacks remain an effective method of stealing credentials and identities, distributing malware, eliciting fraudulent payments etc.
- Research shows that a new phishing site is launched every 20 seconds
- 87% of successful mobile phishing attacks take place outside of e-Mail
- 60% of mobile phishing attacks occur over HTTPS

Hidden Apps

- Hidden apps hide their existence on victim’s devices by removing their icons from the home screen and perform malicious activities
- Hidden apps are the most active mobile threat category in 2019
- Thousands of apps are actively hiding their presence after installation, making them difficult to locate and remove while annoying victims with invasive ads

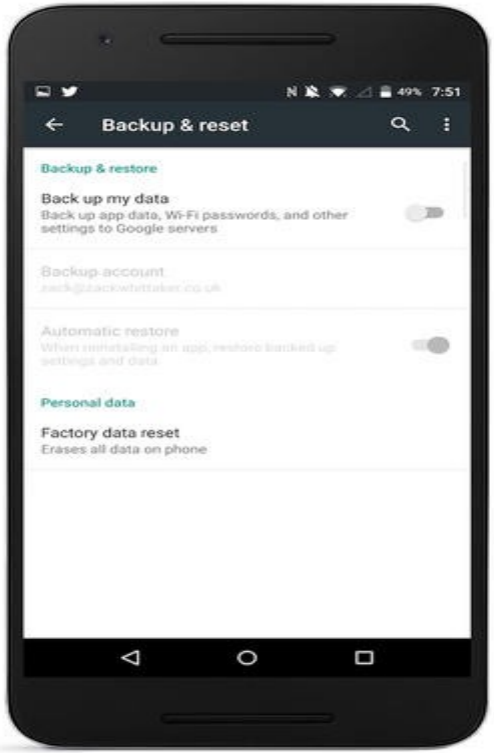
Adware

- Criminals are tricking users into installing adware on their devices that redirects them to a range of different ad types and topics
- Digital ad revenue comes from raw numbers—screens displayed and clicks captured
- Fraudulently increasing these numbers is becoming a very popular technique

Some Important Security & Privacy Configurations in Android

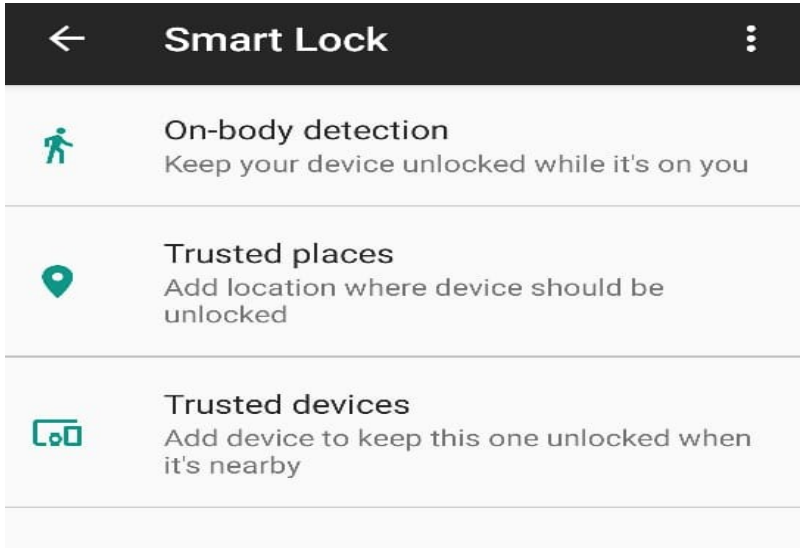
Disable Cloud Based Backup

- The best way to keep your Android phone from sending your personal data to its servers is to turn off backup
- The downside is if you lose your phone, you may lose your data
- But you always have the option to manually back-up to your home computer
- Go to Settings then Backup & Reset, where you can switch off the option to Back up my data


49% 7:51
Backup & reset
Backup & restore
Back up my data
Back up app data, Wi-Fi passwords, and other settings to Google servers
Backup account
Automatic restore
Personal data
Factory data reset
Erases all data on phone

Smart Lock

- Smart Lock aims to keep your data secure without taking a convenience hit
- Go to Settings then Device & Privacy, where you can switch on/ off the option to Smart Lock

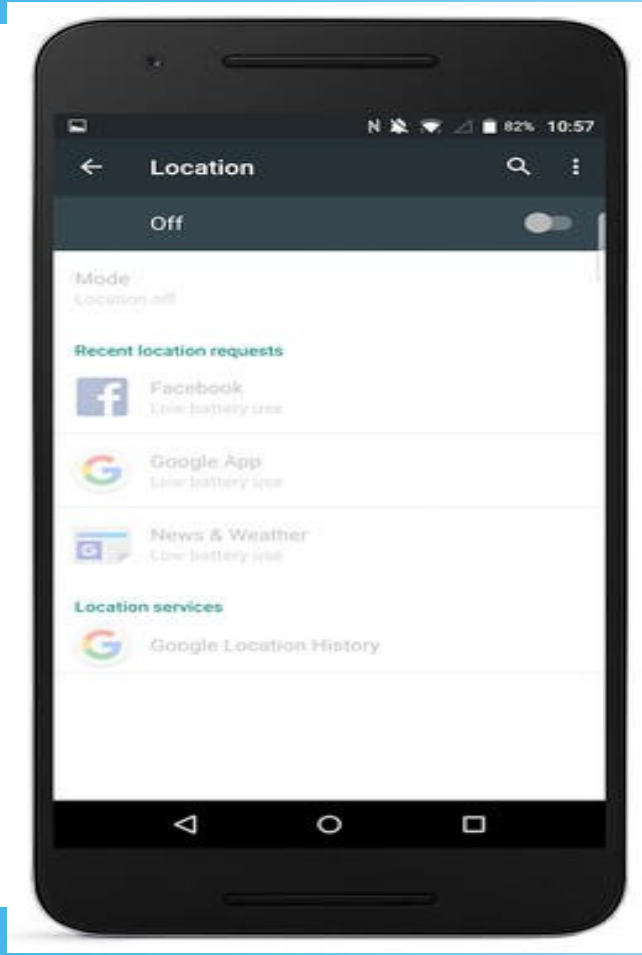

Smart Lock
On-body detection
Keep your device unlocked while it's on you
Trusted places
Add location where device should be unlocked
Trusted devices
Add device to keep this one unlocked when it's nearby

Google’s Advertising Tracking

- Ad-tracking is one of the most pervasive ways for Google and its partners to track your habits.
- Turning off interest-based ads prevents ad networks from building up a profile on what you like and what you don't, based on your viewing, reading, or other habits
- Go to Settings -> Google -> Ads -> Opt out of Ads Personalization which is disabled by default

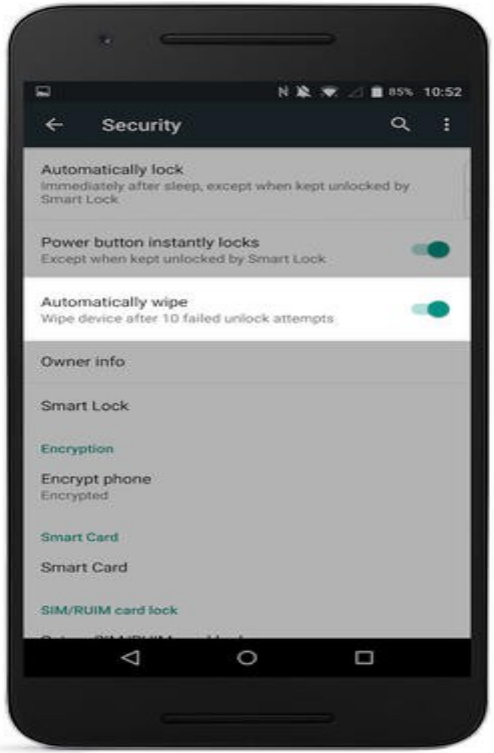
Google’s Location History

- Your location can say a lot about you, such as where you go and even who you meet and what you might do
- Google uses these results to serve more relevant ads and other information. Turning it off can be good for your privacy
- Go to Settings then Location, where you can turn on and off at the top switch. You can also turn off Google Location History by scrolling to the bottom and turning the option off. From here, you can also Delete Location History


82% 10:57
Location
Off
Mode
Location off
Recent location requests
Facebook
Low battery use
Google App
Low battery use
News & Weather
Low battery use
Location services
Google Location History

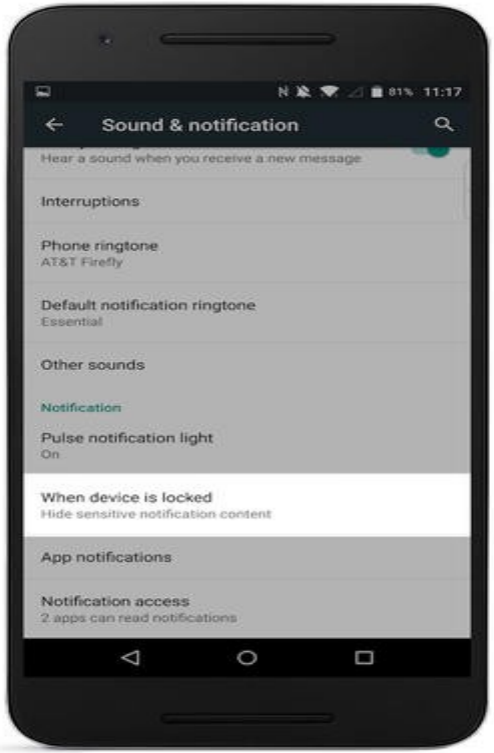
Device Erase Function

- You can enable a setting so that after ten failed unlock attempts, your Android device will be wiped clean and all data destroyed.
- You can turn this setting on from Settings then Security, and then (so long as you have your screen lock enabled), you can turn on the Automatically Wipe setting


85% 10:52
Security
Automatically lock
Immediately after sleep, except when kept unlocked by Smart Lock
Power button instantly locks
Except when kept unlocked by Smart Lock
Automatically wipe
Wipe device after 10 failed unlock attempts
Owner info
Smart Lock
Encryption
Encrypt phone
Encrypted
Smart Card
Smart Card
SIM/RUIM card lock

Lock Screen Notifications

- Your lock screen can show a lot about your life.
- Your Android phone or tablet can limit what's shown on the lock screen in order to prevent others' from seeing your personal content as it comes in
- Go to Settings then Sound & Notifications, and scroll down. You can change how notifications are shown under the When device is locked setting. The most privacy conscious setting is to Hide sensitive notification content so that you know which app is alerting you, without showing its contents


81% 11:17
Sound & notification
Hear a sound when you receive a new message
Interruptions
Phone ringtone
AT&T Firefly
Default notification ringtone
Essential
Other sounds
Notification
Pulse notification light
On
When device is locked
Hide sensitive notification content
App notifications
Notification access
2 apps can read notifications

Prevent unauthorized apps from installing

- Unlike iPhones and iPads, Android devices can run third-party content outside of the Google Play app store.
- This can open up a device to malware attacks.
- The easiest way to ensure that only verified and malware-checked apps can be installed on your phone or tablet is by going to Settings then Security, and ensuring that the Unknown sources option is turned off

Auto-Update

- Make sure to keep your Android device up-to-date
- Ensure that Auto-Update is turned on for auto updation of security patches
- Go to Settings -> Software Update -> Auto Update

How to protect your Smart Phones

- Always update your devices with the latest software
- Especially, install all security patches provided by the OEMs to patch various security threats
- Never visit any shady websites by clicking on the links you have received over SMS, Whatsapp or by any other means
- Beware of social engineering attacks
- Never ever install apps or software from unfamiliar publishers or from third-party app-stores

How to protect your Smart Phones

- Never use public WiFi hotspots for performing critical transactions
- Be vigilant on the applications that you install on your device and the permissions they seek from you
- Be vigilant on the amount of data and battery being consumed by your applications
- Uninstall unused applications from your device on a regular basis
- Use a good Anti-Virus solution to secure your mobile device.

References

- https://www.mcafee.com/content/dam/consumer/en-us/docs/2020-Mobile-Threat-Report.pdf
- https://www.wandera.com/files/mobilethreatlandscapereport2020wpvoebwoncaz/mobile-threat-landscape-report-2020-page-5/
- https://www.hindustantimes.com/tech/smartphones-hotspots-of-cyberattacks-in-india-check-point/story-zJQDykref5bqH4lDYFkAMO.html
- https://www.zdnet.com/pictures/android-phone-tablet-privacy-security-settings/15/

Thank You