Securing Android Devices

Sun City Computer Club

Seminar Series

May 2021

Revision 1

To view or download a MP4 file of this seminar With audio

- Audio Recording of this seminar
- Use the link above to access MP4 audio recording

Where are Android Devices?

- Smart Phones
- Smart Tablets
- Smart TVs
- E-Book Readers
- Game consoles
- Music players
- Home phone machines
- Video streamers – Fire, Chromecast,

Why Android devices?

- Cutting edge technology – Google
- User Friendly
- User modifications

  Android Software Development Kit (SDK) Open Source
- Huge volume of applications
- Google, Samsung, LG, Sony, Huawei, Motorola, Acer, Xiaomi, …
- 2003
- CUSTOMIZABLE

My Choices

- Convenience vs Privacy
- Helpful <-> Harmful
- Smart devices know more about us than we do

Android “flavors” flavours

- Android versions and their names
- Android 1.5: Android Cupcake
- Android 1.6: Android Donut
- Android 2.0: Android Eclair
- Android 2.2: Android Froyo
- Android 2.3: Android Gingerbread
- Android 3.0: Android Honeycomb
- Android 4.0: Android Ice Cream Sandwich
- Android 4.1 to 4.3.1: Android Jelly Bean
- Android 4.4 to 4.4.4: Android KitKat
- Android 5.0 to 5.1.1: Android Lollipop
- Android 6.0 to 6.0.1: Android Marshmallow
- Android 7.0 to 7.1: Android Nougat
- Android 8.0 to Android 8.1: Android Oreo
- Android 9.0: Android Pie
- Android 10

Many potential combinations

- Each manufacturer “tunes” the Android release to suit

#1 Keep up with updates

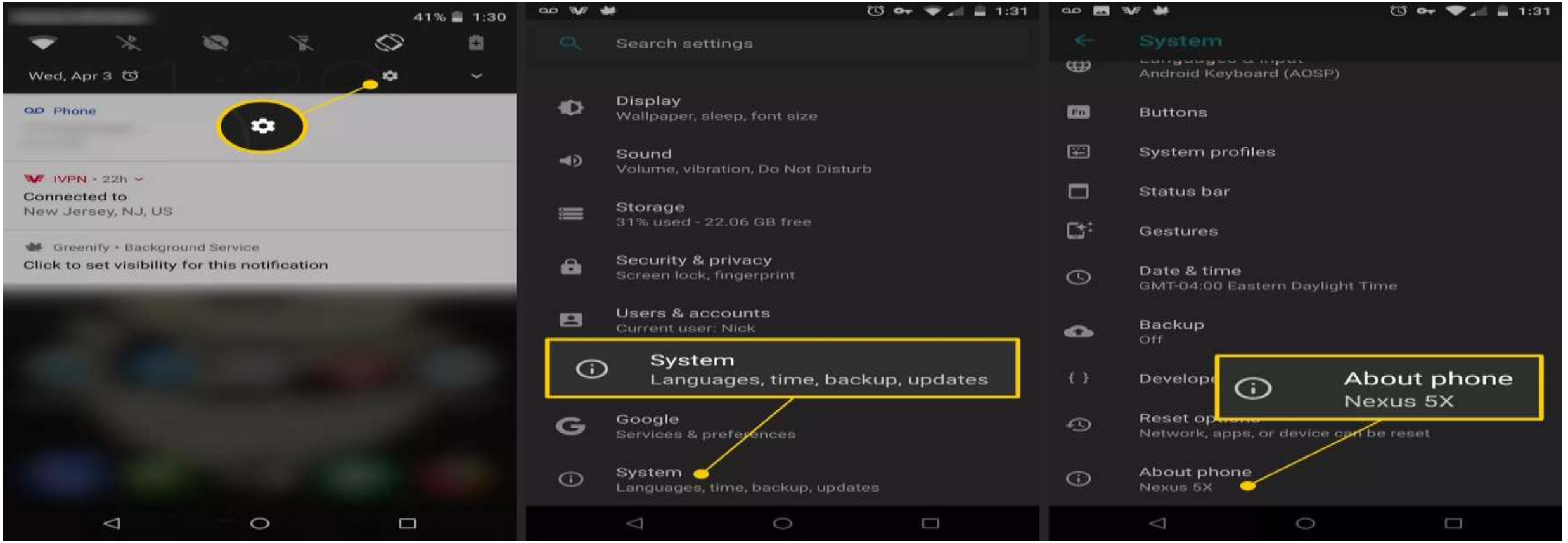
Android Operating System

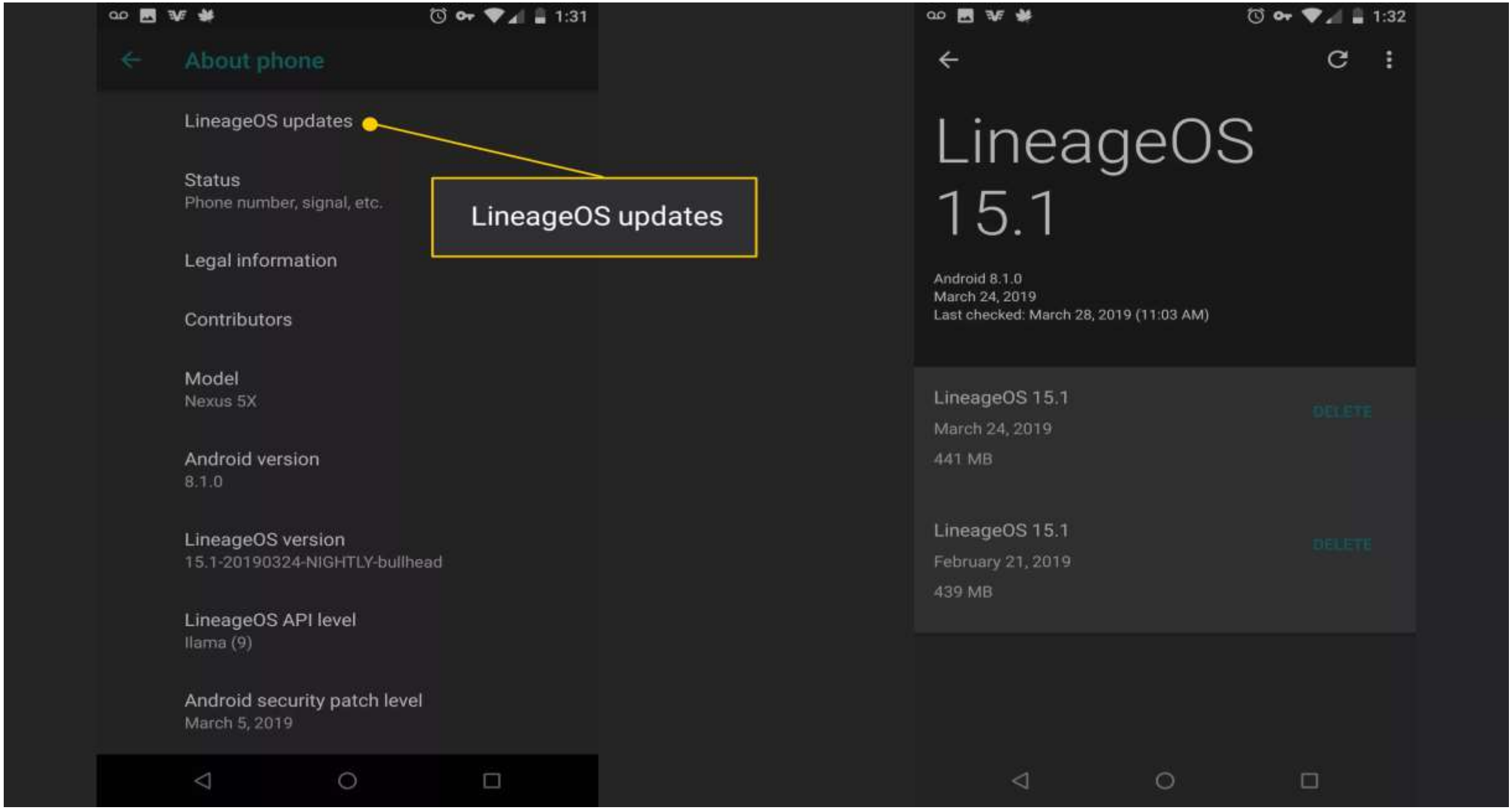
Android firmware (Very vendor specific)

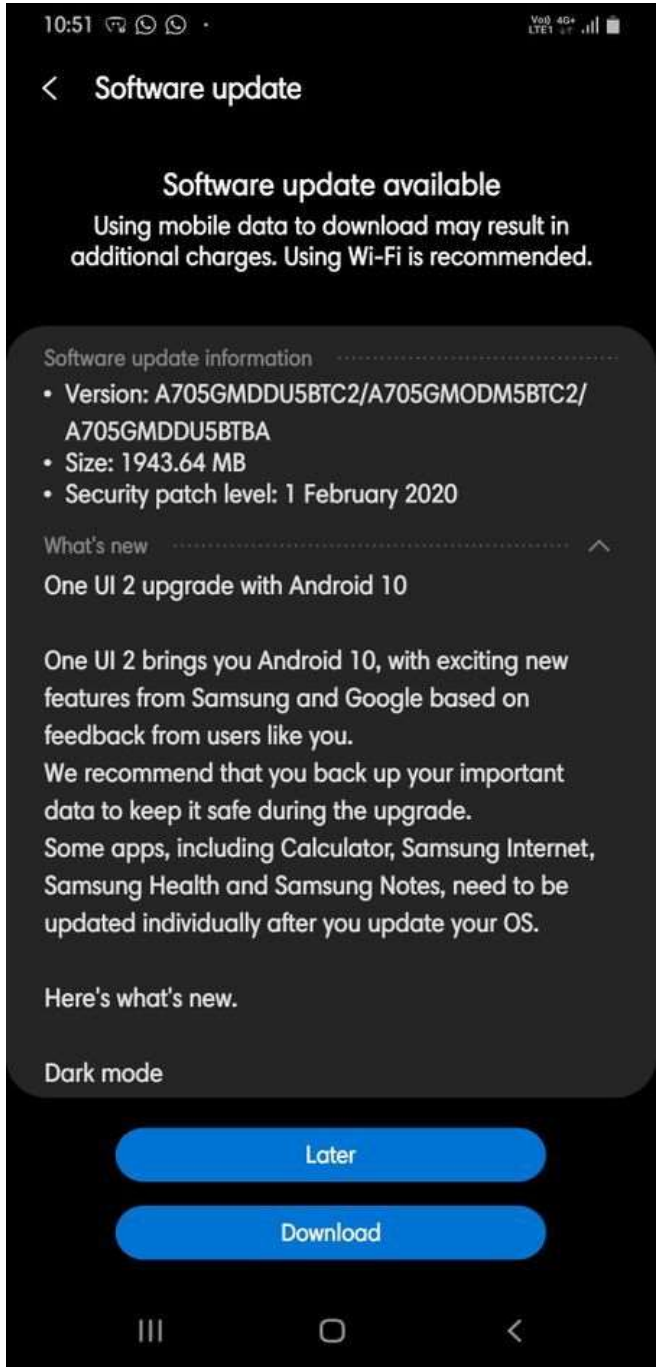
Android Applications (Apps)
Android settings

Android Update

- Settings (gear icon) -> System – Advanced – System Update – Check




1:31
About phone
LineageOS updates
Status
Phone number, signal, etc.
Legal information
Contributors
Model
Nexus 5X
Android version
8.1.0
LineageOS version
15.1-20190324-NIGHTLY-bullhead
LineageOS API level
llama (9)
Android security patch level
March 5, 2019
LineageOS updates
1:32
LineageOS 15.1
Android 8.1.0
March 24, 2019
Last checked: March 28, 2019 (11:03 AM)
LineageOS 15.1
March 24, 2019
441 MB
DELETE
LineageOS 15.1
February 21, 2019
439 MB
DELETE


10:51
Software update
Software update available
Using mobile data to download may result in additional charges. Using Wi-Fi is recommended.
Software update information
• Version: A705GMDDU5BTC2/A705GMODM5BTC2/ A705GMDDU5BTBA
• Size: 1943.64 MB
• Security patch level: 1 February 2020
What's new
One UI 2 upgrade with Android 10
One UI 2 brings you Android 10, with exciting new features from Samsung and Google based on feedback from users like you.
We recommend that you back up your important data to keep it safe during the upgrade.
Some apps, including Calculator, Samsung Internet, Samsung Health and Samsung Notes, need to be updated individually after you update your OS.
Here's what's new.
Dark mode
Later
Download

BEWARE FAKEs

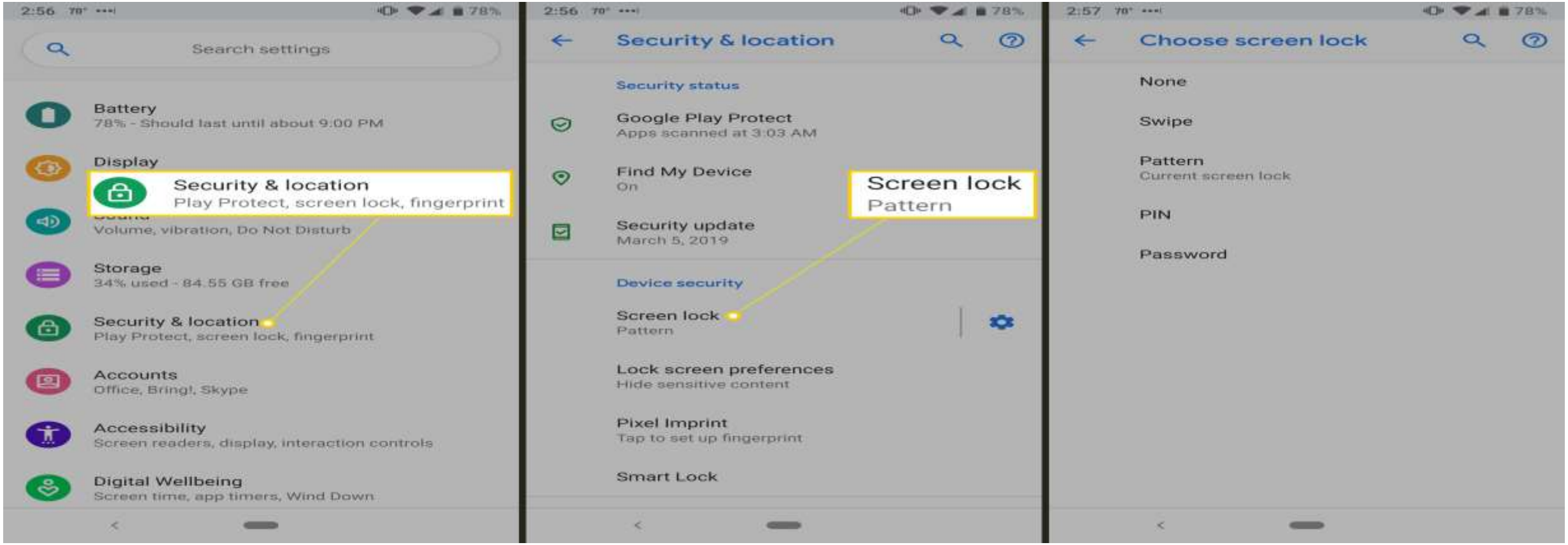
Check, then double Check

- Do not load Android updates from Links, Popups, eMail, …
- Verify at Vendor’s site


Settings

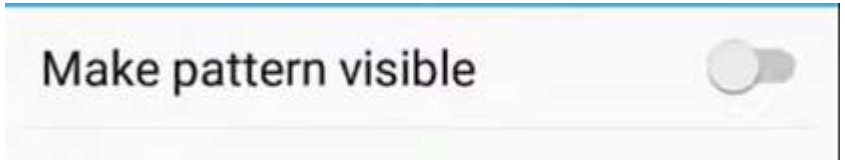
Enable Screen Lock

- Settings – Security – Device Security – Screen Lock



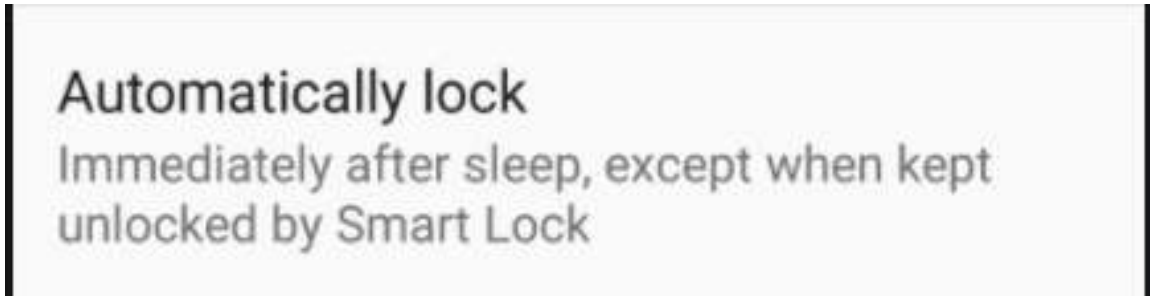
Pattern invisible ?

- Shoulder surfing
- Physical traces on screen
- UV light
- 7-year-old
- Your paranoid level
- Loss of visual feedback



Immediately lock device as soon as it is set to sleep

- Known attacks against sleep – Lock lag
- Settings – Security – Device security – Screen lock



Power button instantly locks

- Power button device to sleep

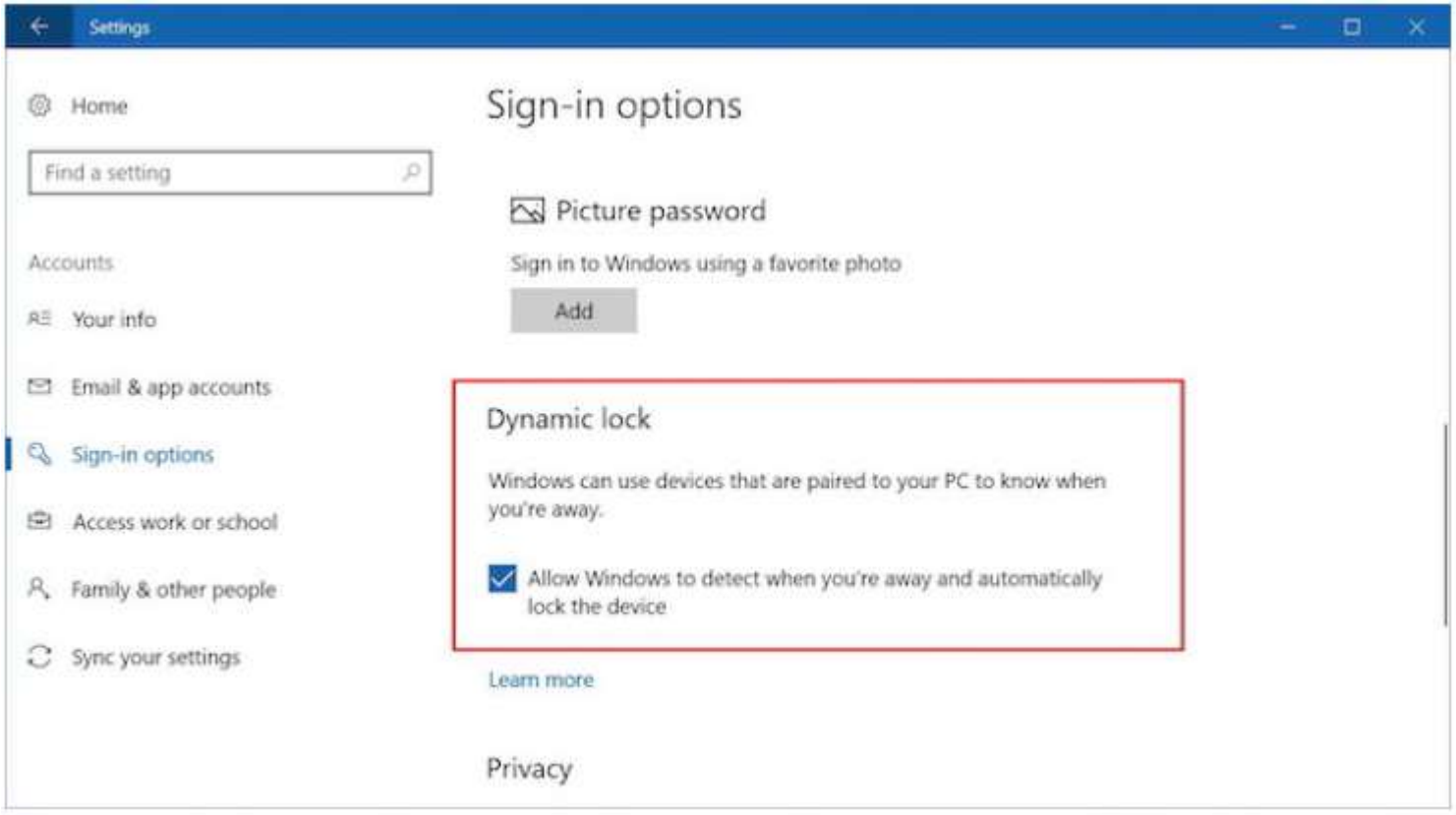
  Adds Power button locks as well

Time out Smart Lock?

- On-body detection
  Keep device unlocked while it is on you
- Trusted places
  Add location where device should be unlocked
- Trusted Devices
  Add device to keep this one unlocked when it’s nearby
- Trusted face
  Device will unlock when face is recognized
- Trusted voice
  setup voice recognition
- Chromebook
  Better together

Microsoft Windows - Dynamic Lock

- Android and other Bluetooth devices



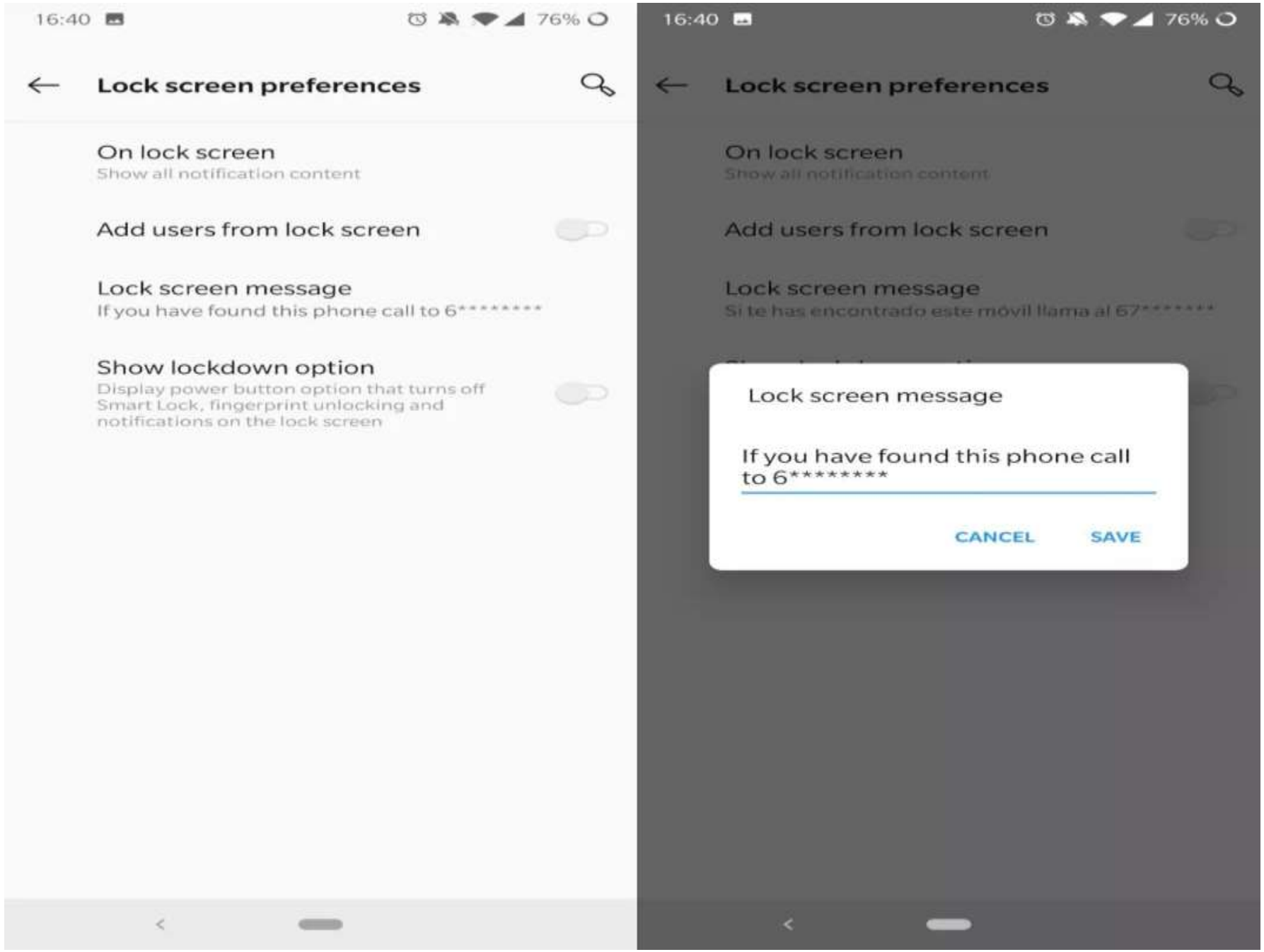
Lock Screen Message

- Deterrent warning
- Device recognition without need to unlock
- Emergency information

If found, Please call xxx-xxx-xxxx

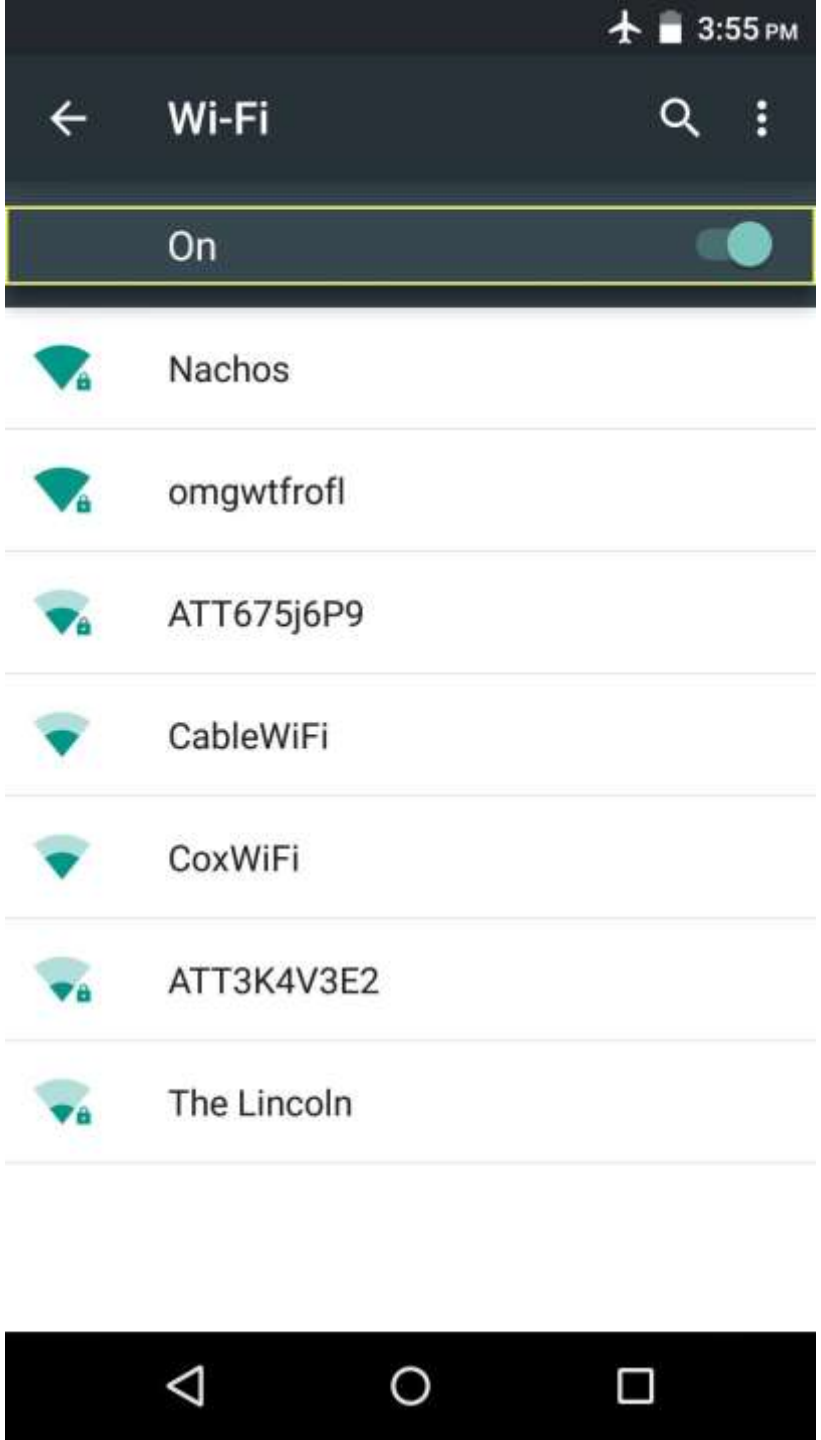
Settings – Display – Advanced – Lock screen display

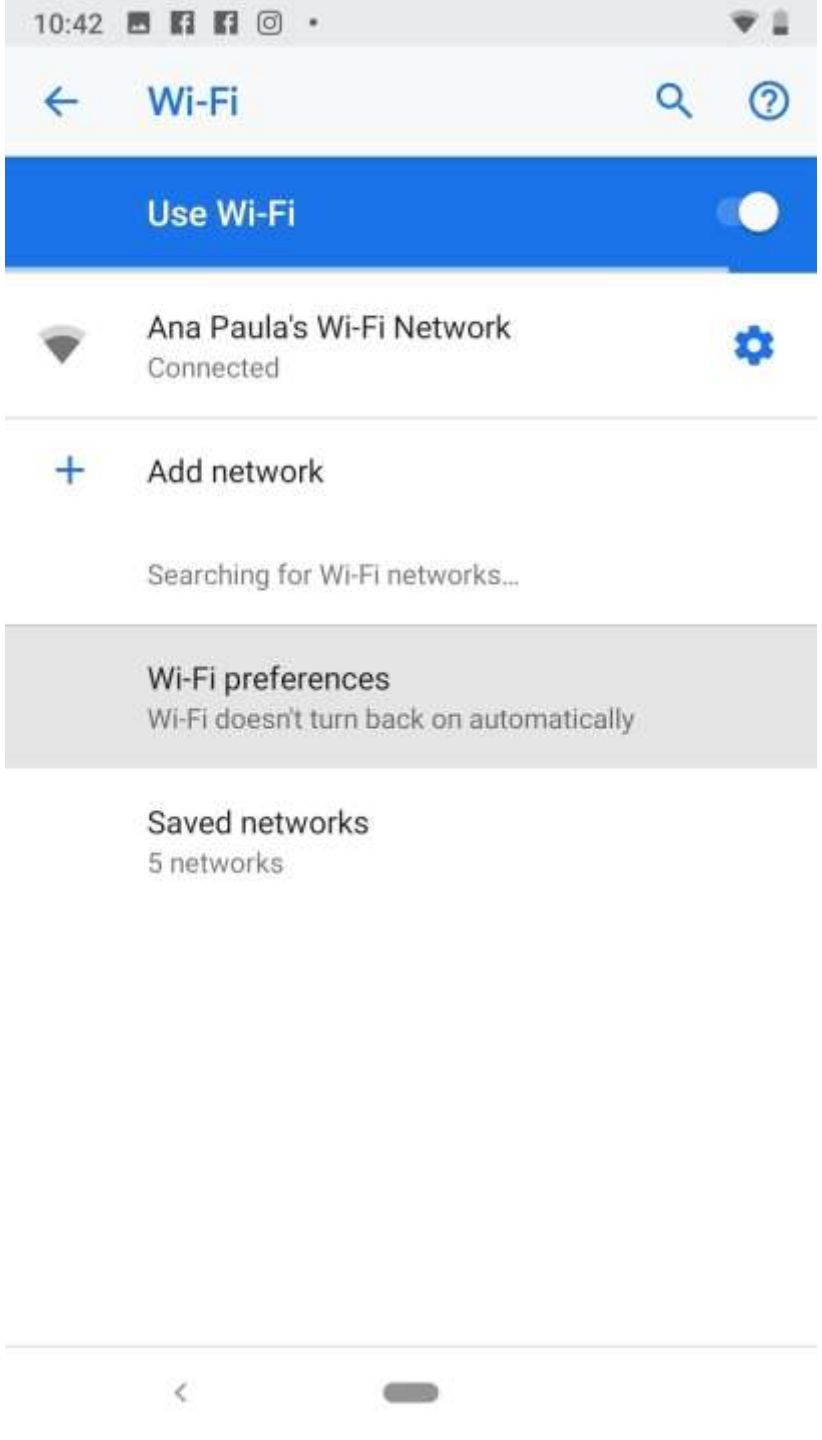
Lock screen message

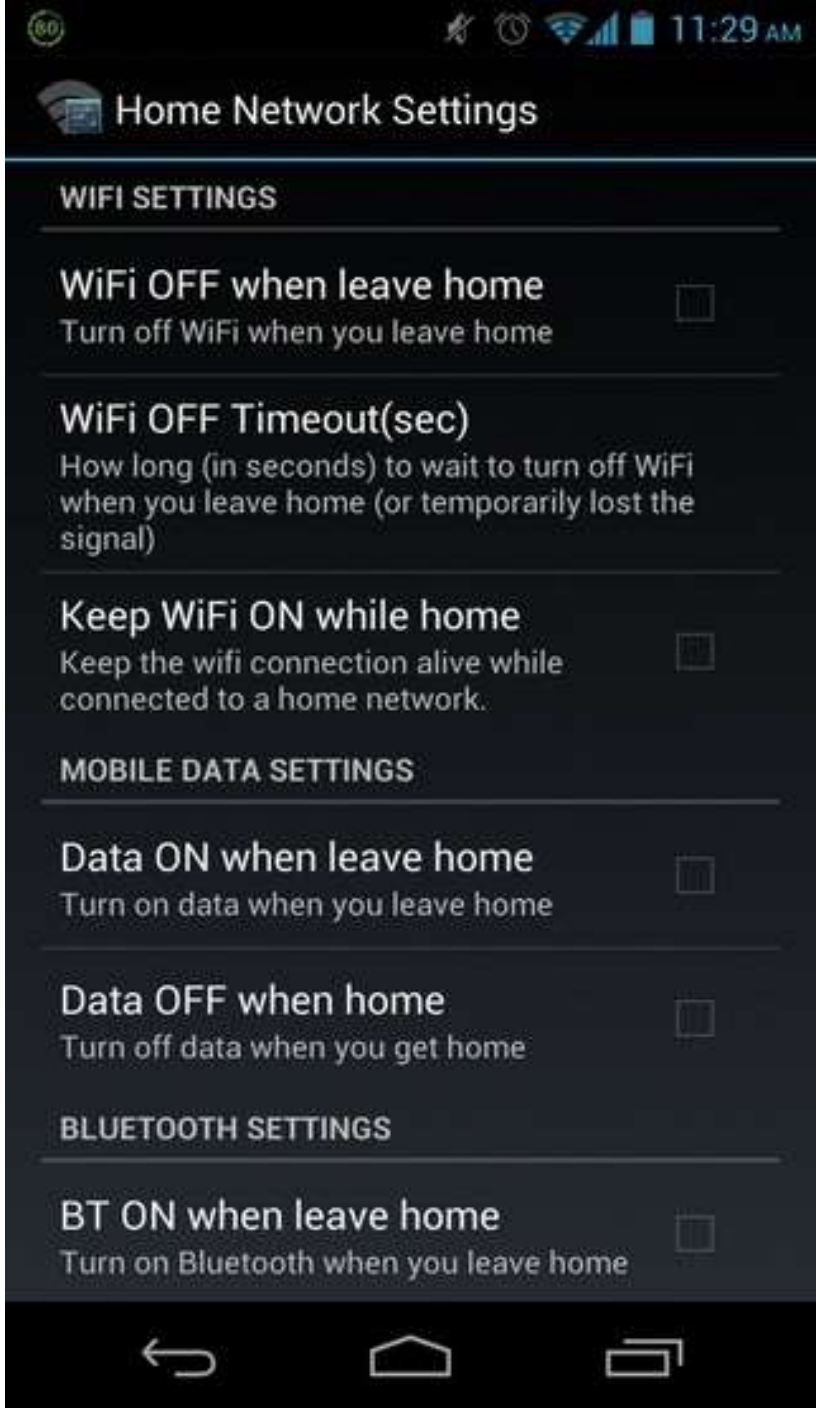

16:40
76%
Lock screen preferences
On lock screen
Show all notification content
Add users from lock screen
Lock screen message
If you have found this phone call to 6********
Show lockdown option
Display power button option that turns off Smart Lock, fingerprint unlocking and notifications on the lock screen
16:40
76%
Lock screen preferences
On lock screen
Show all notification content
Add users from lock screen
Lock screen message
Si te has encontrado este móvil llama al 67********
Lock screen message
If you have found this phone call to 6********
CANCEL
SAVE

Do Not connect to untrusted Wi-Fi networks

- Cellular more difficult to sniff
- Cellular is point-to-point with encryption
- Wi-Fi beacon


3:55 PM
Wi-Fi
On
Nachos
omgwtfrofl
ATT675j6P9
CableWiFi
CoxWiFi
ATT3K4V3E2
The Lincoln


10:42
Wi-Fi
Use Wi-Fi
Ana Paula's Wi-Fi Network
Connected
Add network
Searching for Wi-Fi networks...
Wi-Fi preferences
Wi-Fi doesn't turn back on automatically
Saved networks
5 networks


11:29 AM
Home Network Settings
WIFI SETTINGS
WiFi OFF when leave home
Turn off WiFi when you leave home
WiFi OFF Timeout(sec)
How long (in seconds) to wait to turn off WiFi when you leave home (or temporarily lost the signal)
Keep WiFi ON while home
Keep the wifi connection alive while connected to a home network.
MOBILE DATA SETTINGS
Data ON when leave home
Turn on data when you leave home
Data OFF when home
Turn off data when you get home
BLUETOOTH SETTINGS
BT ON when leave home
Turn on Bluetooth when you leave home

CAUTIONS

- CELLULAR, WI-FI, BLUETOOTH, NFC, ETC. ARE **RADIO**
- **A BROADCASTER (YOUR DEVICE)**
- **MANY RECEIVERS (*ANYONE* IN RANGE)**
- **WI-FI HAS NETWORK NAMES**
- **WI-FI CAN HAVE ENCRYPTION**
  WEP, WPA, WPA2, WPA3
- **LOWEST COMMON DENOMINATOR**
- **ONLY DATA PORTION IS ENCRYPTED**
- **BROADCASTER ID IS UNENCRYPTED**

CAUTIONS

- SPOOFING – ATTACKER SETS THEIR ADDRESS, ETC.
- DISASSOCIATE – ATTACKER SETS THEIR ADDRESS THE SAME AS YOURS
- QUITE EASILY DONE THAT INFORMATION SENT UNENCRYPTED

CAUTIONS

- YOUR DEVICE ASSOCIATES AND SAVES HOME NETWORK
- YOU LEAVE HOME NETWORK
- YOUR DEVICE BEACONS HOME NETWORK
- ATTACKER SEES HOME NETWORK BEACONS
- ATTACKER SETS THEIR NETWORK NAME TO BE HOME NETWORK
- OPTION- SEND DISASSOCIATE
- YOUR DEVICE ASSOCIATES WITH ATTACKER

CAUTIONS

- BEACONS FOR ANY/ALL SAVED NETWORK NAMES
- HOME NETWORK HOLIDAY INN I HOP
- YOUR DEVICE HAS YOUR LIFE PLUS
- YOUR DEVICES HAS YOUR CONTACTS

- MOST APPLICATIONS CAN USE CELLULAR
- THUS, CONSIDER WI-FI OFF
- WHEN NEEDED, UPDATES, …

‘Show passwords’ set to ‘disabled’

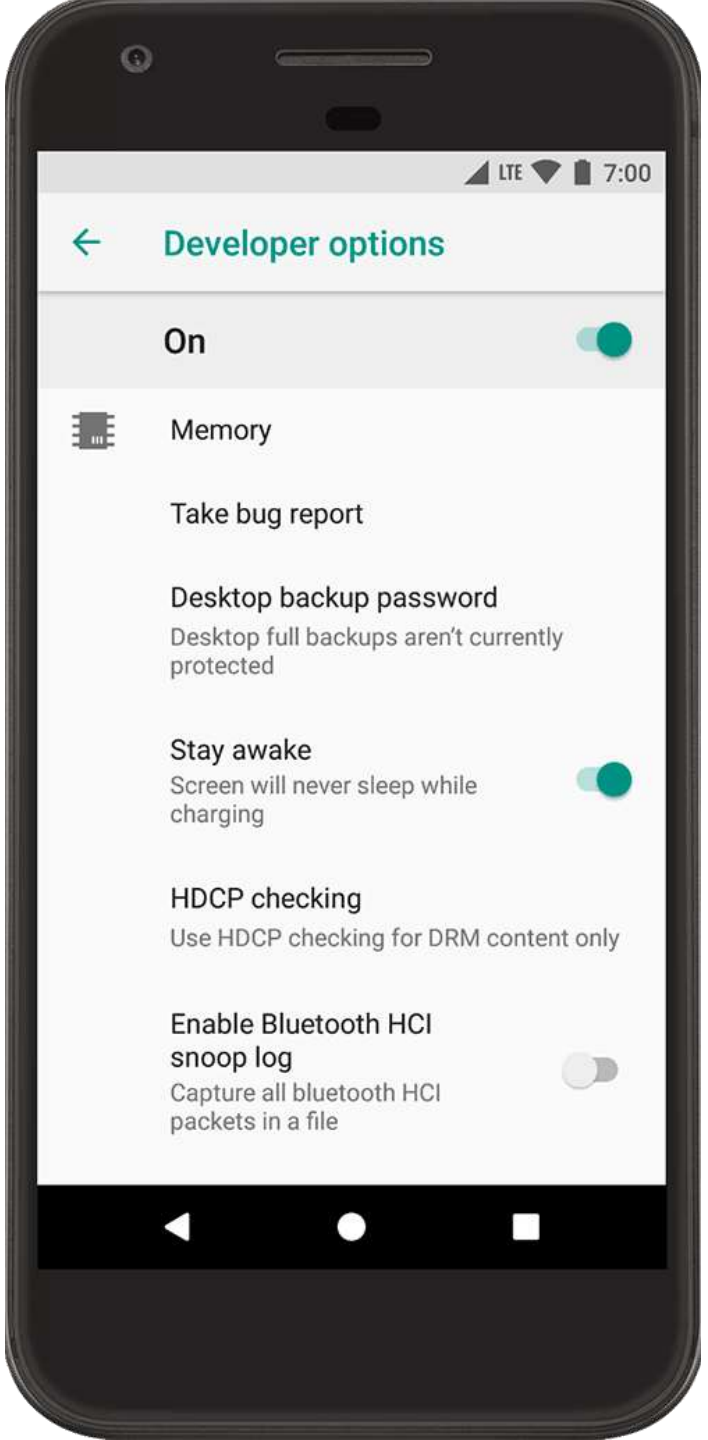
- Shoulder surfing
- Video surveillance

- Small screen small keyboard bright sunlight …

Settings – privacy – Show passwords to off

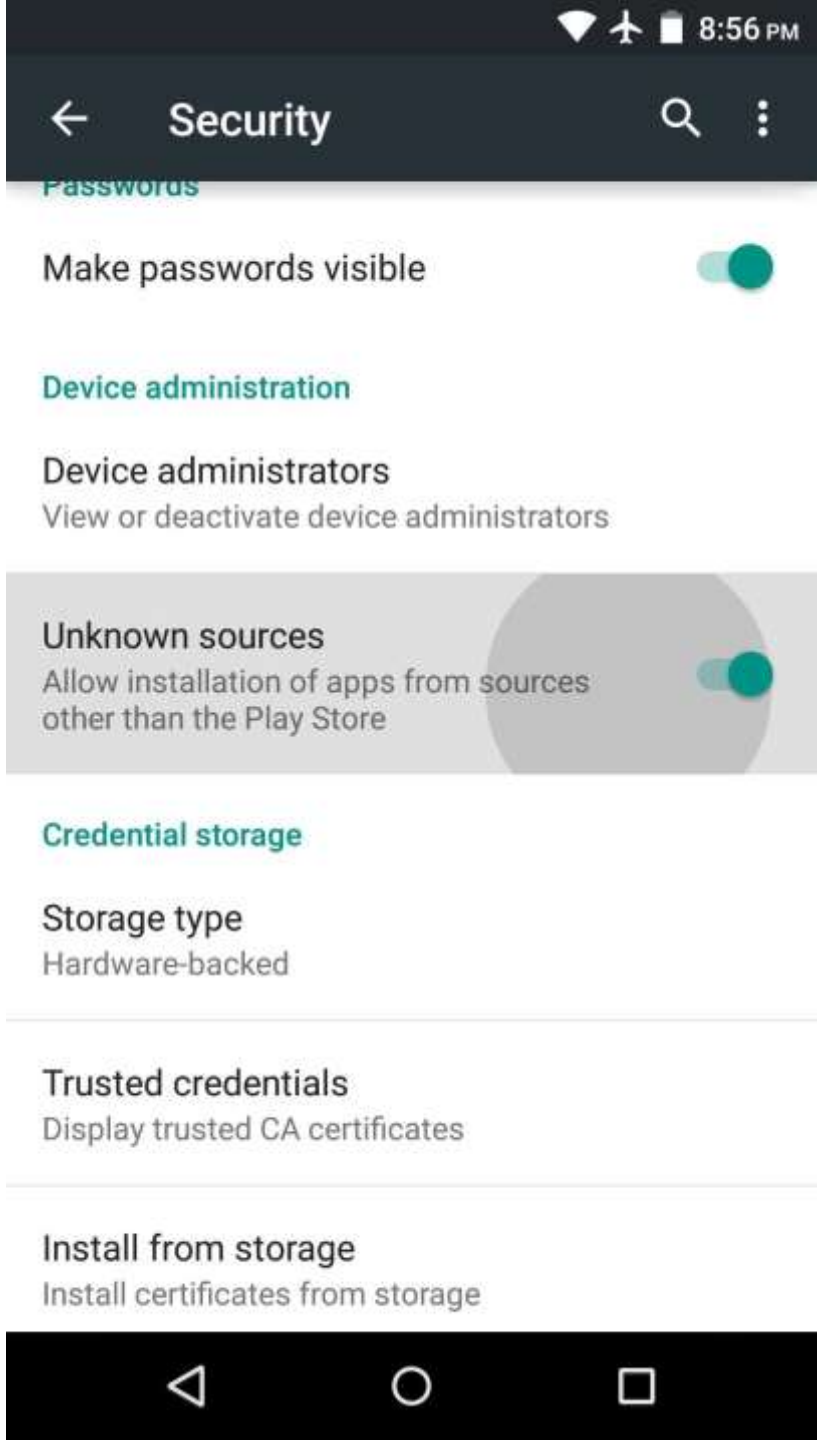
Developer Options

- Usually not needed
- Default should be disabled
- Settings – System – Advanced – Developer Options

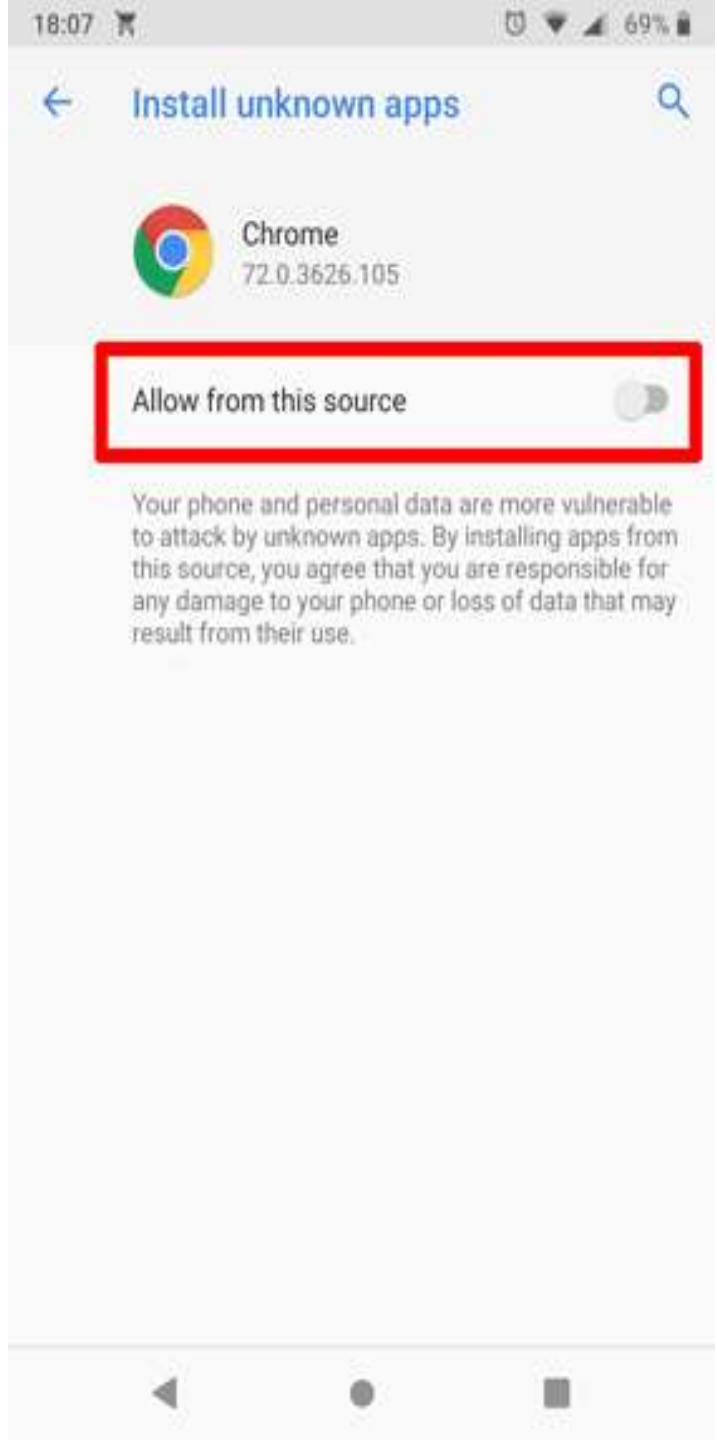


Install unknown apps

- Google Play *mostly safe*
- Security vetted, malicious intent NOT vetted
- Updates to apps not usually vetted
- Apps sold *then* made malicious or creepy
- Settings – Apps & notifications – Advanced – Special app access


8:56 PM
Security
Passwords
Make passwords visible
Device administration
Device administrators
View or deactivate device administrators
Unknown sources
Allow installation of apps from sources other than the Play Store
Credential storage
Storage type
Hardware-backed
Trusted credentials
Display trusted CA certificates
Install from storage
Install certificates from storage


26% 11:32
More settings
Device administrators
Encryption and credentials
Install apps from external sources
Allow HiSuite to use HDB
HDB lets you connect your device to a computer (HiSuite) without using USB debugging mode.
Revoke HiSuite's HDB authorizations
manyandroid.app
Trusted agents
View or deactivate trusted agents.
Device identifier
Usage information access
Screen pinning
Off

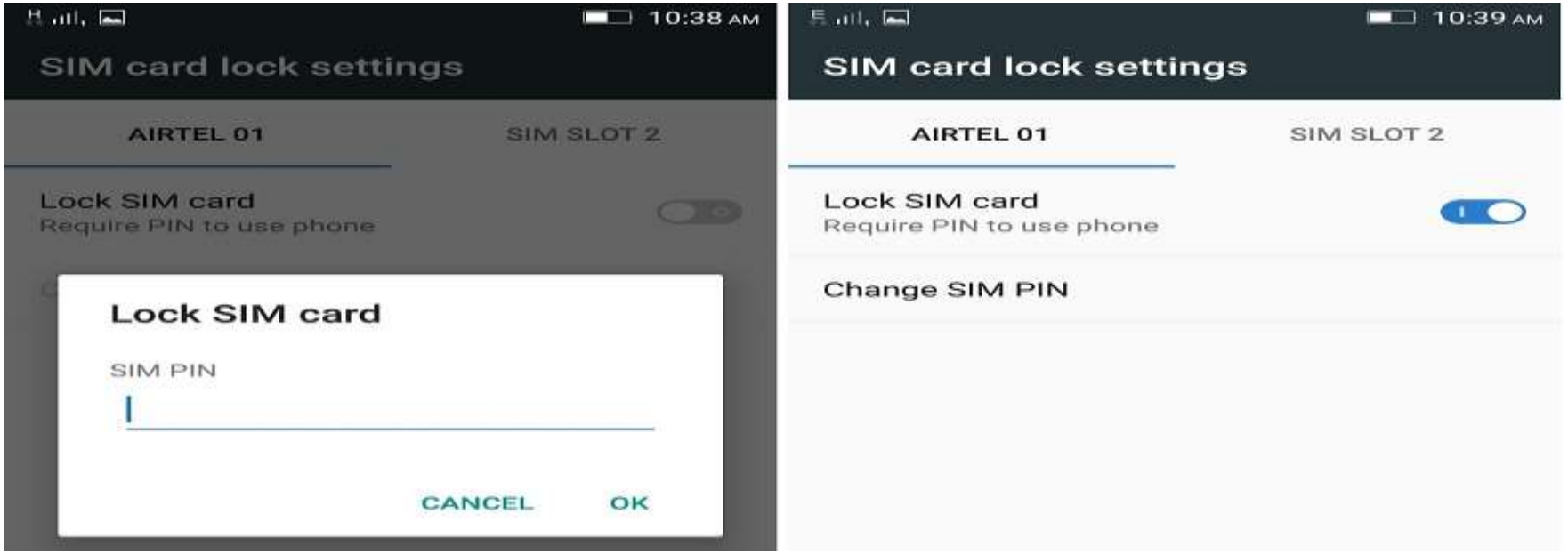

18:07
69%
Install unknown apps
Chrome
72.0.3626.105
Allow from this source
Your phone and personal data are more vulnerable to attack by unknown apps. By installing apps from this source, you agree that you are responsible for any damage to your phone or loss of data that may result from their use.

Root the device

- “root” removed/bypasses protections
- Check with manufacturer
- Root checkers can root the device, report the device is not rooted
- https://www.wikihow.tech/Check-if-Your-Android-Cellphone-Is-Rooted-or-Not
- https://www.wikihow.com/Unroot-Android

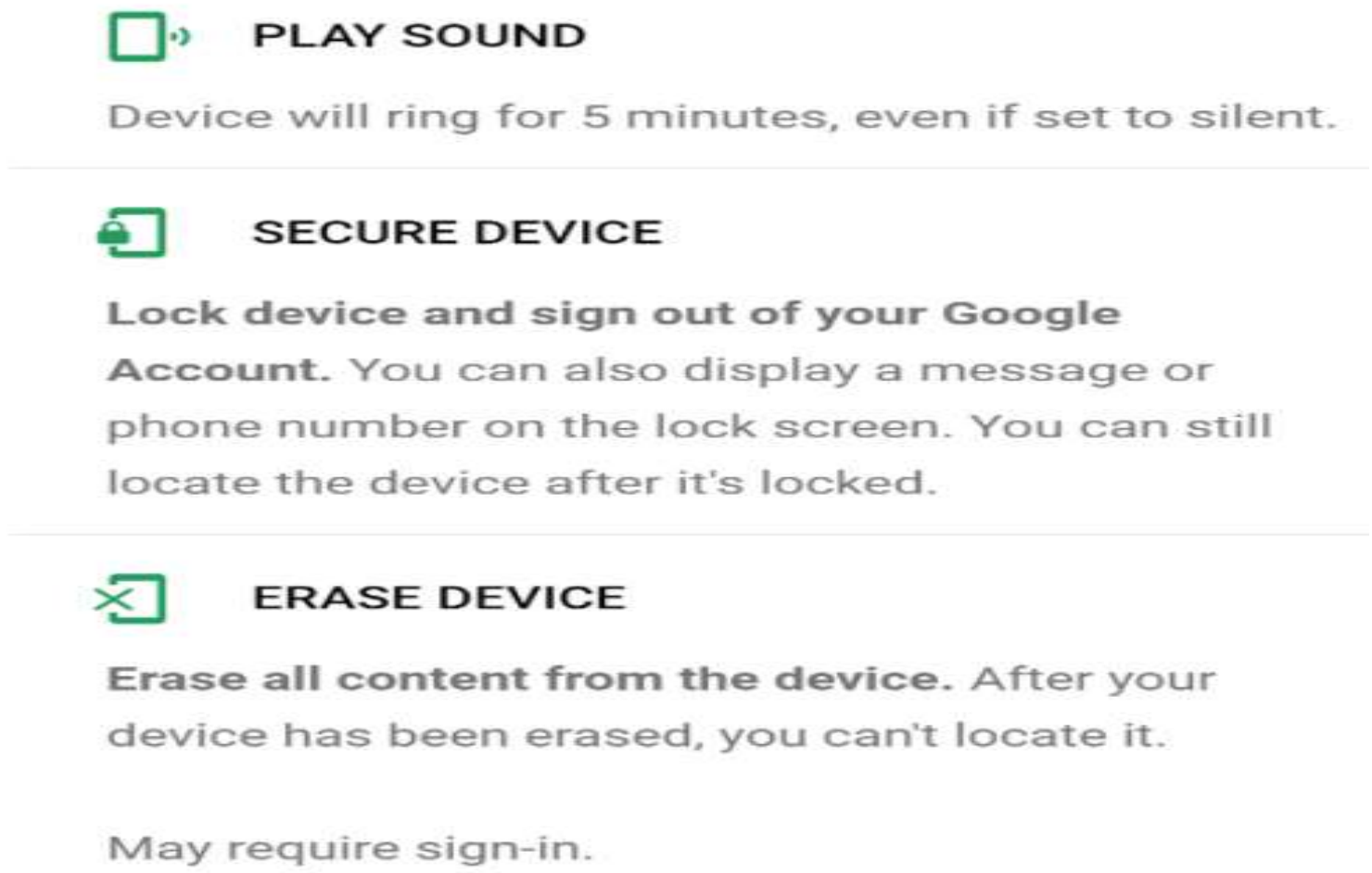
Lock SIM card(s)

- PIN to unlock
- Prevents re-use of SIM card in another device
- SIM cards can hold contacts, messages, etc.
- Only devices NOT locked by service provider can lock SIM card
- Universally known



Enable ‘Find My Device”

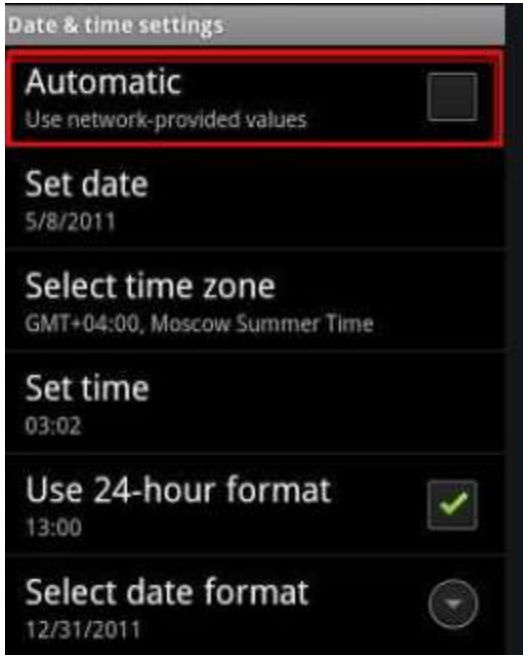
- Settings – Security – SECURITY STATUS – Find My Device
- Locate device
- Remote lock
- Erase



‘Use network-provided time’
‘Use network-provided time zone’

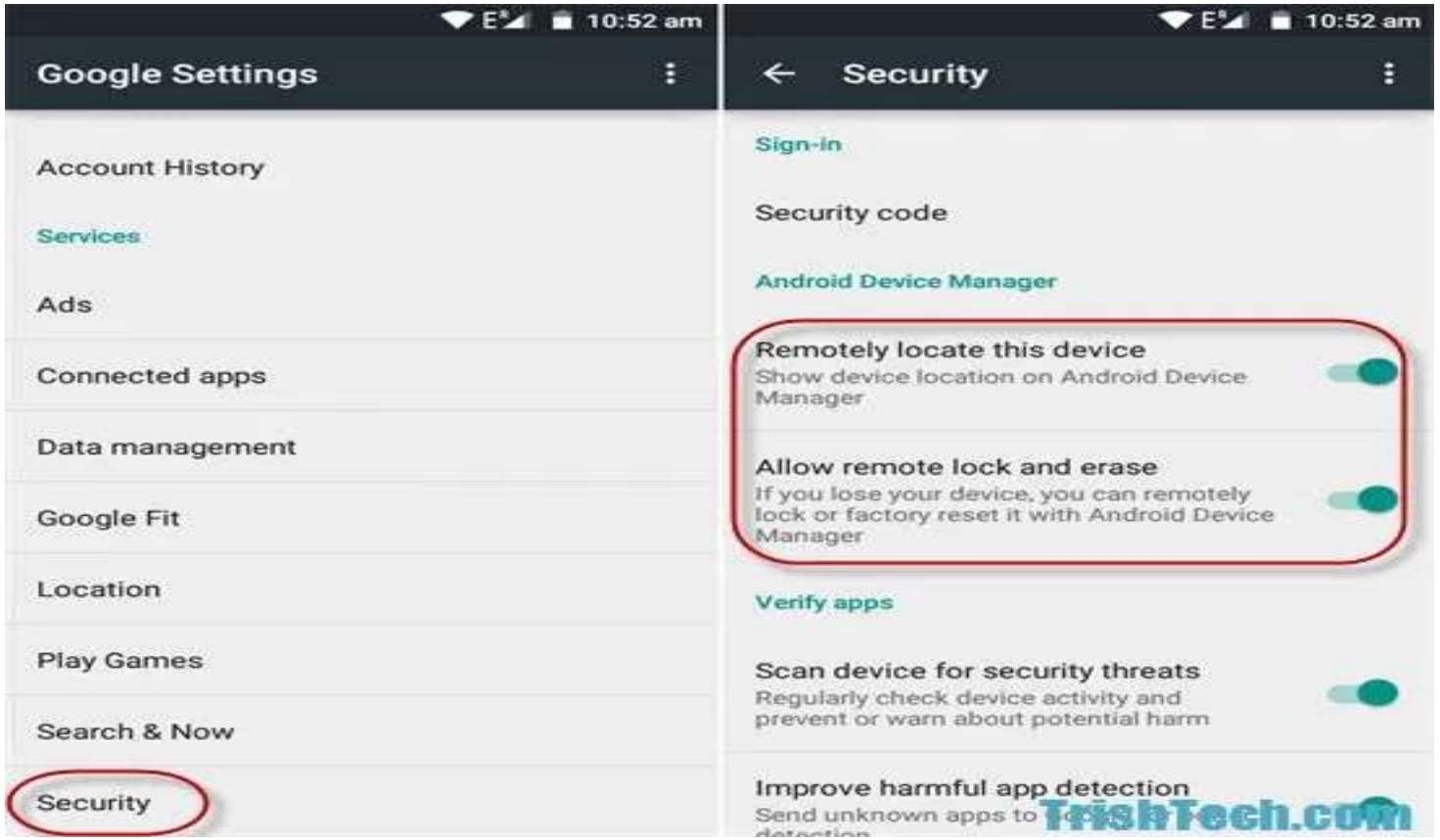
- Automated, more accurate
- Help with forensics, synchronize logs, device recovery

Settings – System – Date & time



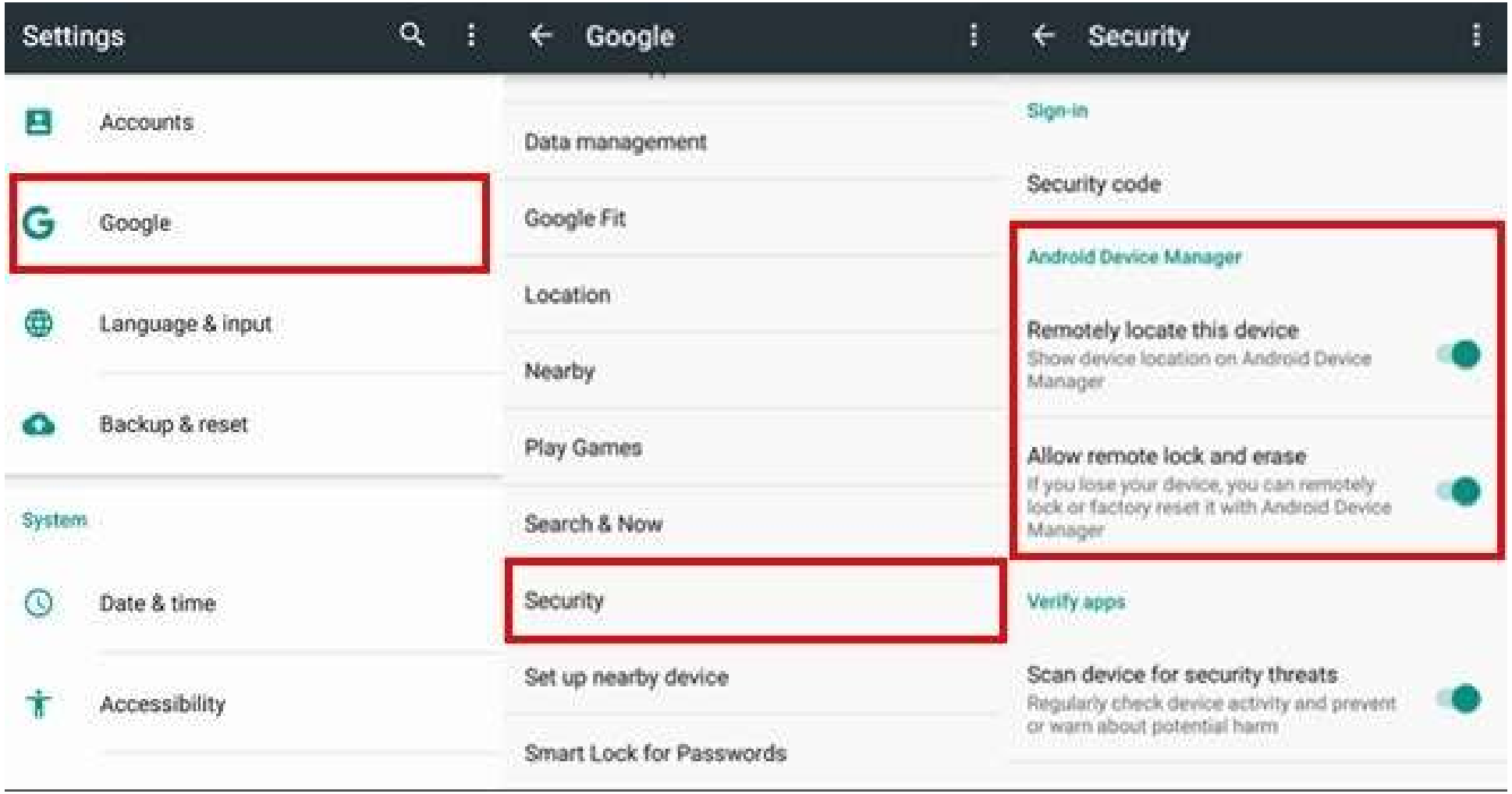
‘Remotely locate this device’

- Settings – Google – Services – Security – Find My Device
- *Google tracking Location Services*



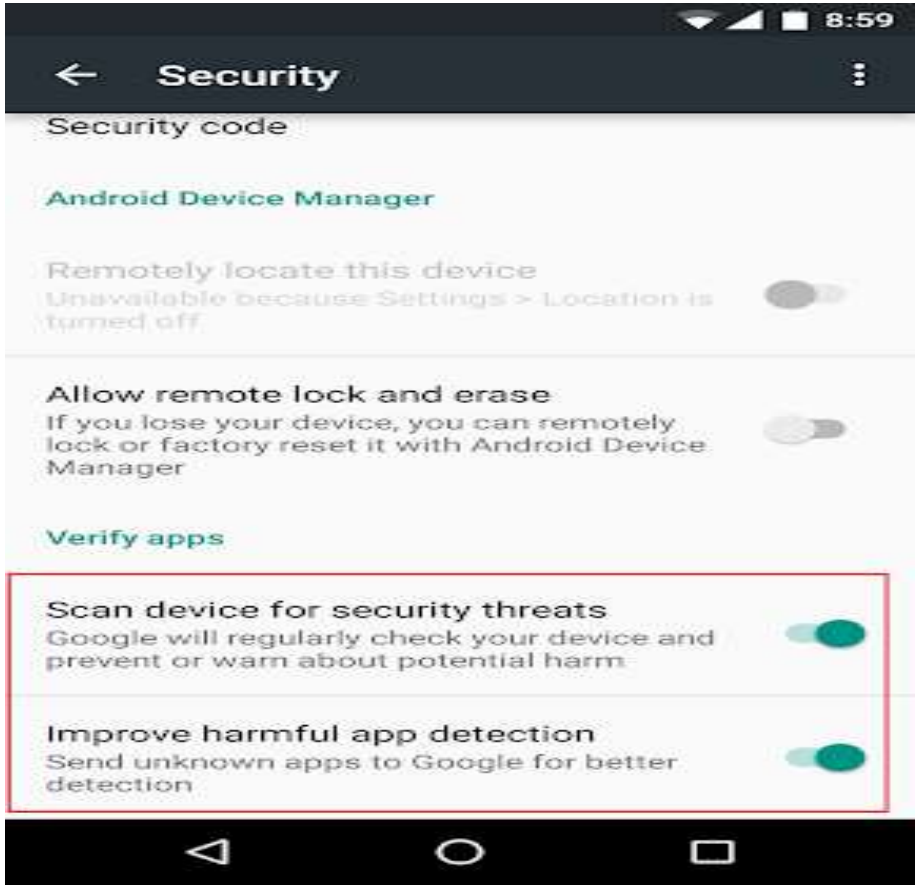
Allow remote lock and erase

- Settings – Security – DEVICE SECURITY – Device admin apps



Scan device for security threats

- Settings – Google – Services – Security – Security status – Google Play Protect – Settings
- Let Google



Harmful app detection

- Helpful

  Early detection of harmful app loading, installation

  Patient 0

  A lag between loading and warning

- Harmful

  No control of which apps are loaded to Google

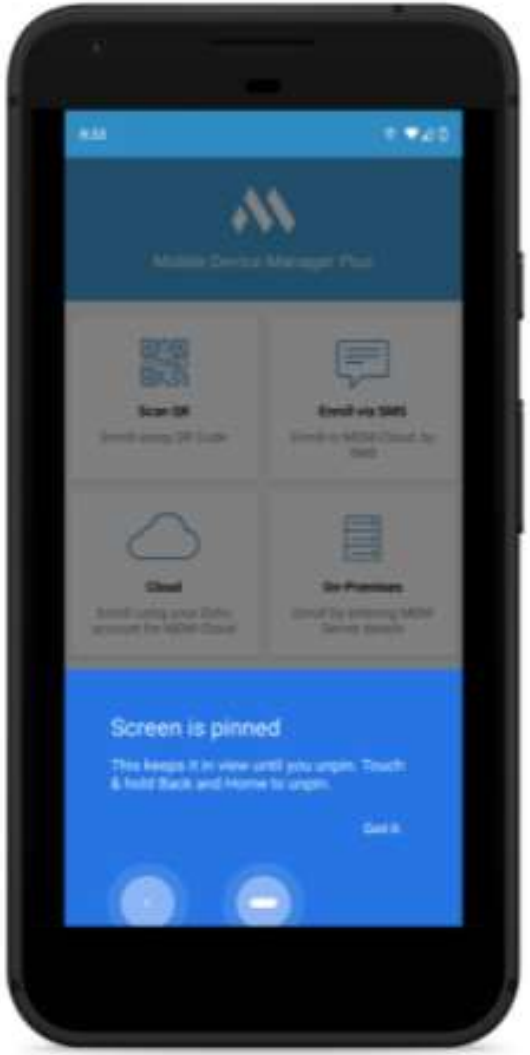
  Your private app loading activity is loaded

Ask for unlock pattern/PIN/password before unpinning

- Another person usage
- Screen pinning
- Locks users to a particular screen
- Android Guided Access
- Settings – Security – Advanced – Screen Pinning

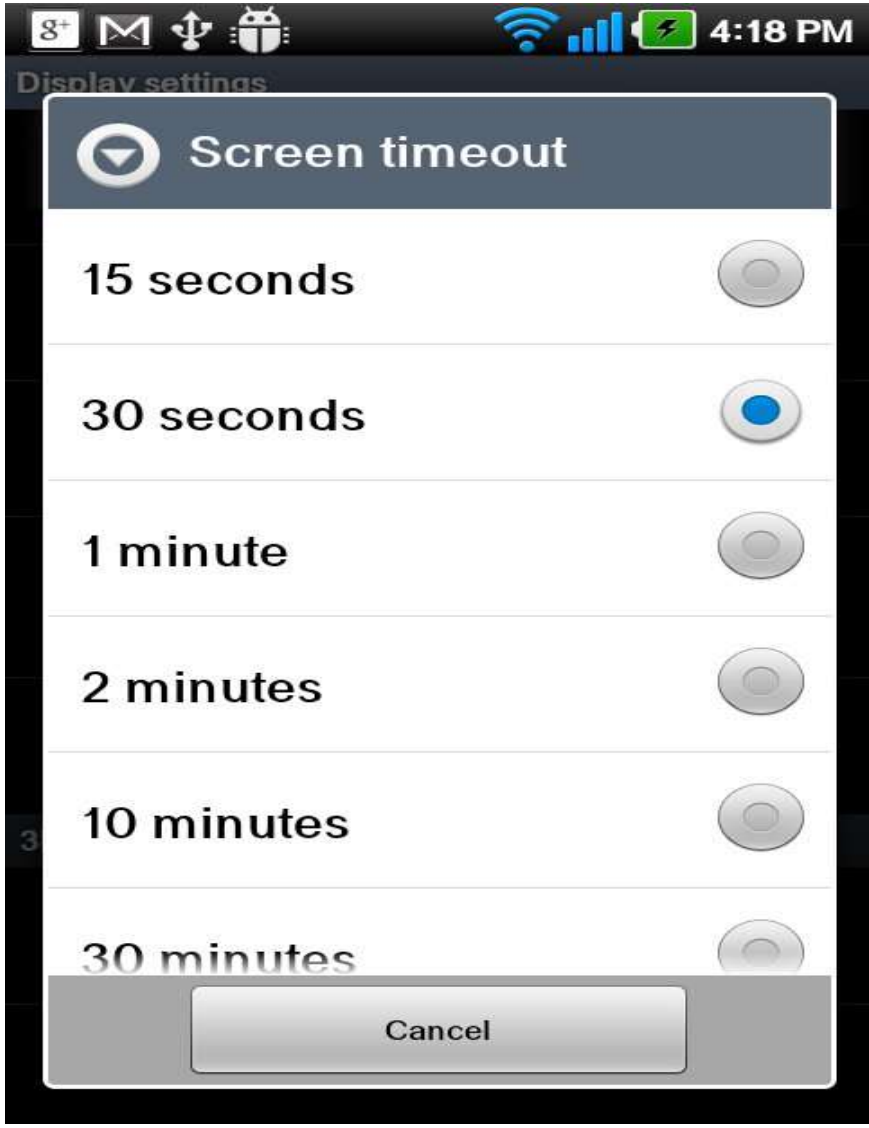
Android Screen Pinning

- Navigate to desired screen, Select app, click on Pin



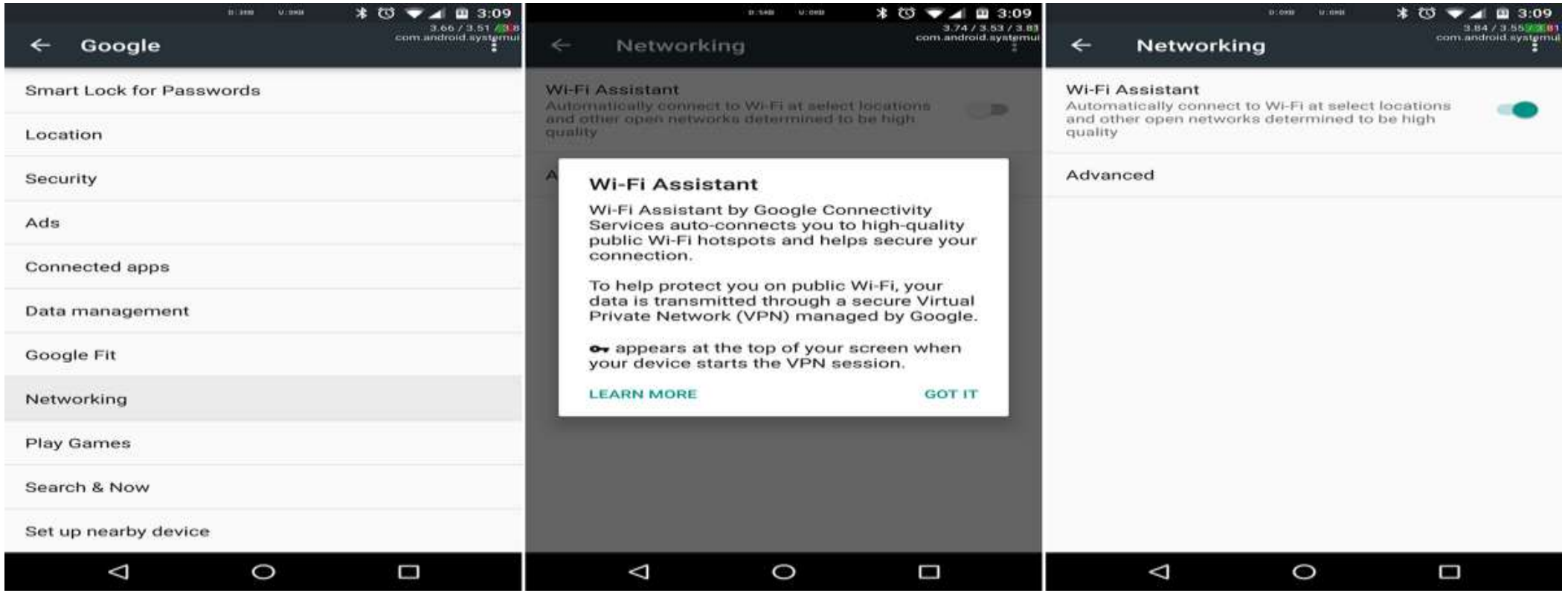
Screen timeout ‘1 minute or less’

- Quick Theft
- Settings – Display – Advanced – Screen timeout



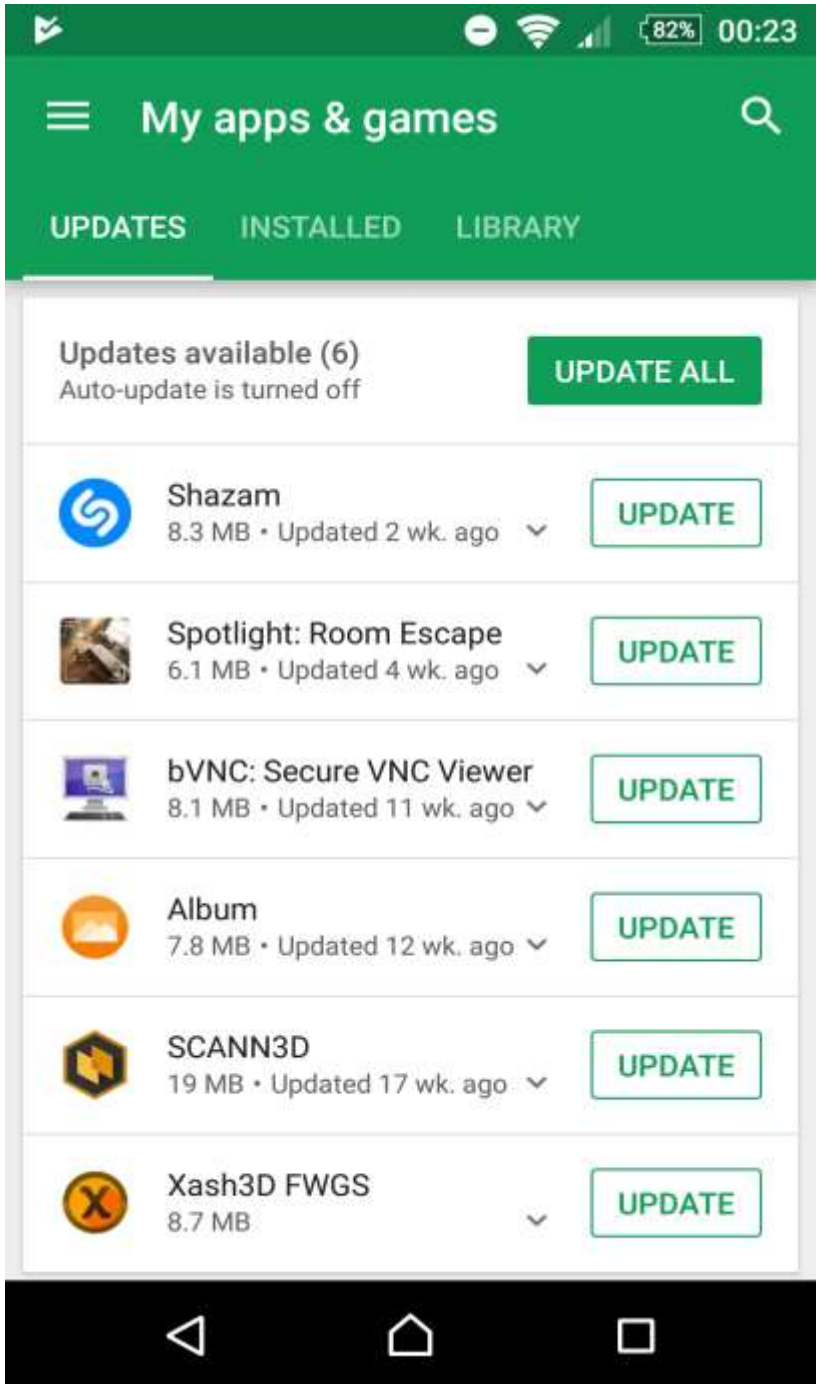
Wi-Fi assistant set to Disabled

- Automatically connect to ANY open Wi-Fi and tunnel through Google VPN servers
- Settings – Google – Services – Networking – Wi-Fi assistant OFF



Keep device Apps Up to date

- Play Store from Launcher
- Menu – My apps & Games

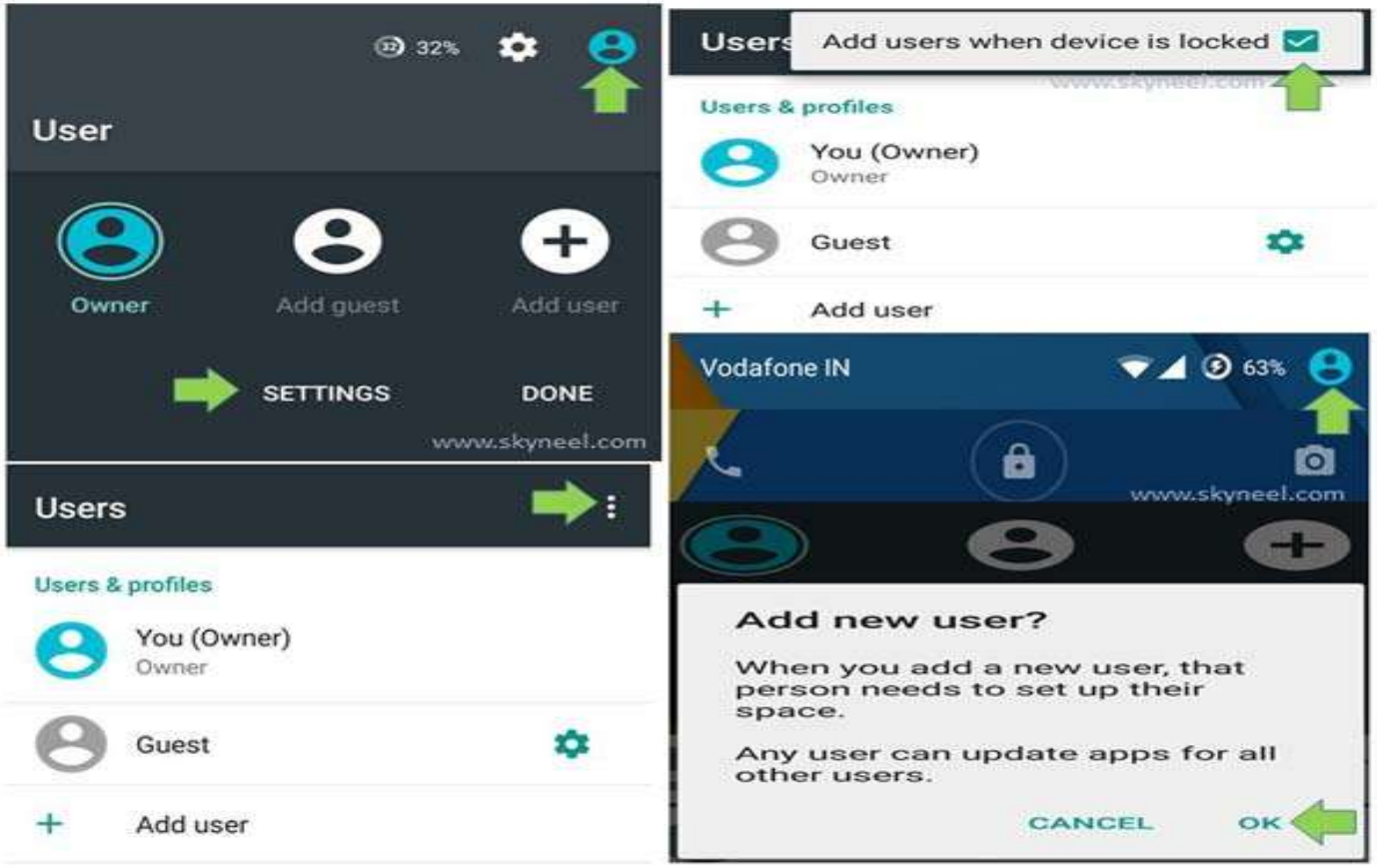


Keep device Apps Up to date

- Apps loaded outside Play Store
- Security suite app updates
- Security suite signatures

Add users from lock screen Disabled

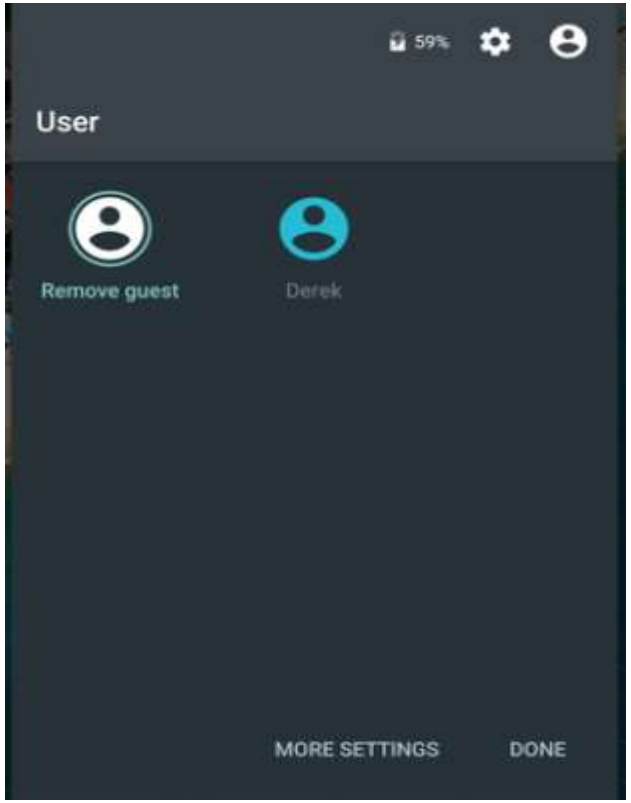
- Users and Guest can do most owner tasks
- Wi-Fi and Bluetooth connections shared
- Settings – System – Advanced – Multiple users – Add users from lock screen



Ensure Guest profiles no NOT exist

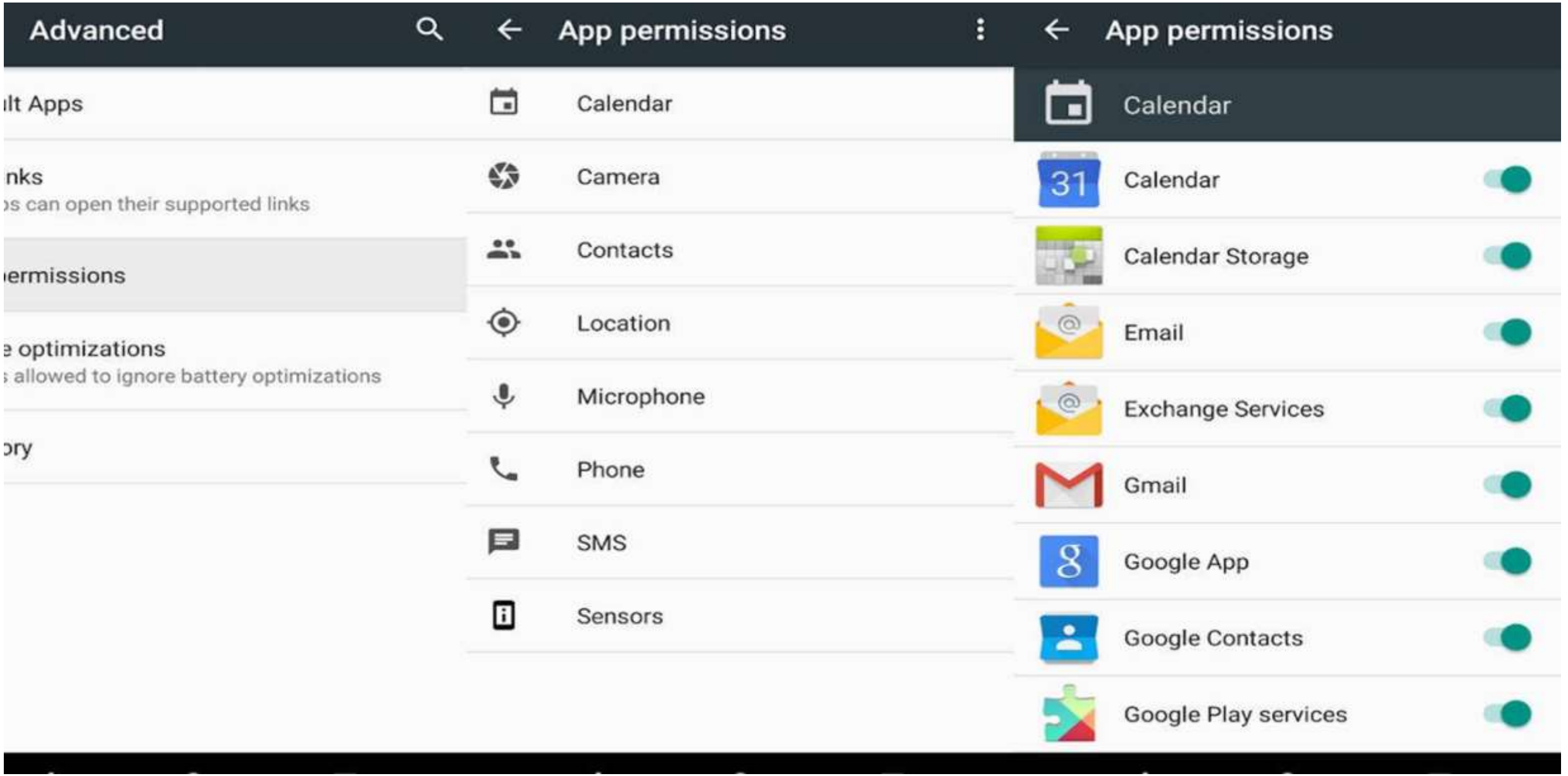
- Settings – System – Advanced – Multiple Users

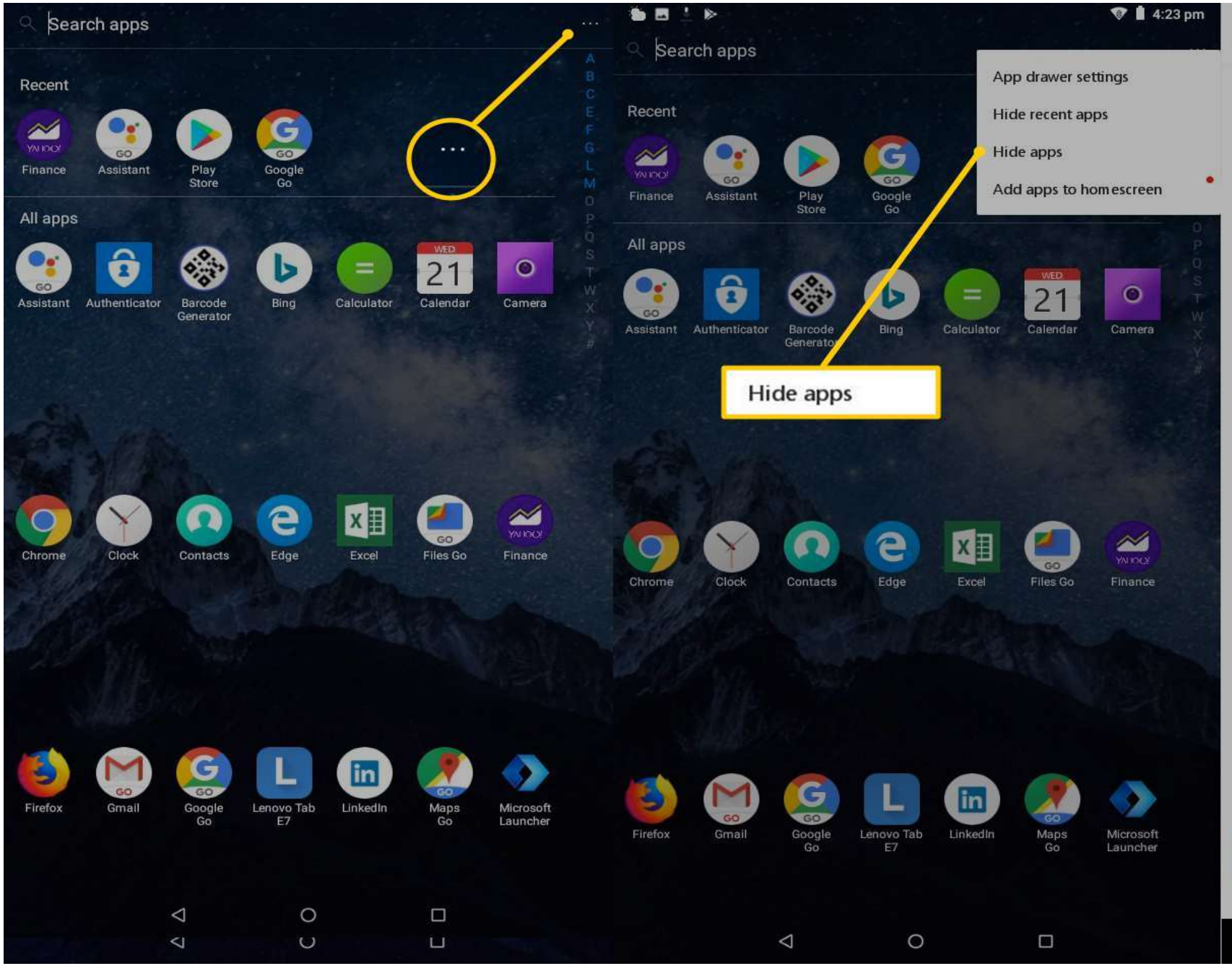
  Guests grayed out
- Quick Settings – Profile – Guest profile – Remove guest – Remove



Review device app’s permissions regularly

- Settings – Apps and notifications – See all apps
- Permissions more granular
- Apps MAY disfunction with revoking permissions


Advanced
lt Apps
nks
s can open their supported links
ermissions
e optimizations
s allowed to ignore battery optimizations
ory
App permissions
Calendar
Camera
Contacts
Location
Microphone
Phone
SMS
Sensors
App permissions
Calendar
Calendar
Calendar Storage
Email
Exchange Services
Gmail
Google App
Google Contacts
Google Play services


Search apps
Recent
Finance
Assistant
Play Store
Google Go
All apps
Assistant
Authenticator
Barcode Generator
Bing
Calculator
Calendar
Camera
Chrome
Clock
Contacts
Edge
Excel
Files Go
Finance
Firefox
Gmail
Google Go
Lenovo Tab E7
LinkedIn
Maps Go
Microsoft Launcher

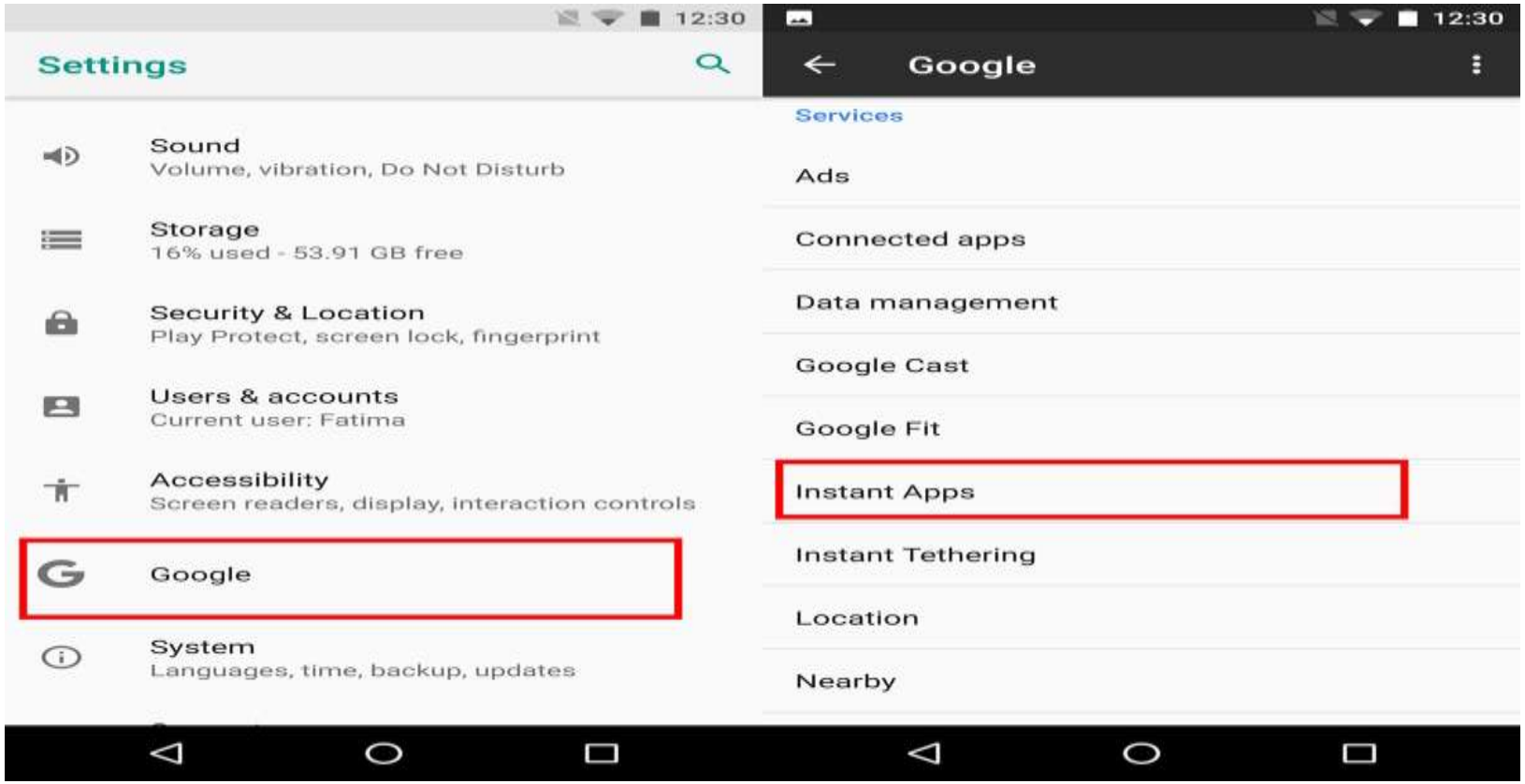
4:23 pm
Search apps
App drawer settings
Hide recent apps
Hide apps
Add apps to homescreen
Recent
Finance
Assistant
Play Store
Google Go
All apps
Assistant
Authenticator
Barcode Generator
Bing
Calculator
Calendar
Camera
Hide apps
Chrome
Clock
Contacts
Edge
Excel
Files Go
Finance
Firefox
Gmail
Google Go
Lenovo Tab E7
LinkedIn
Maps Go
Microsoft Launcher


4:24 pm
Hidden apps
Investing
UNHIDE
Hide apps

‘Instant apps’ set to ‘Disabled’

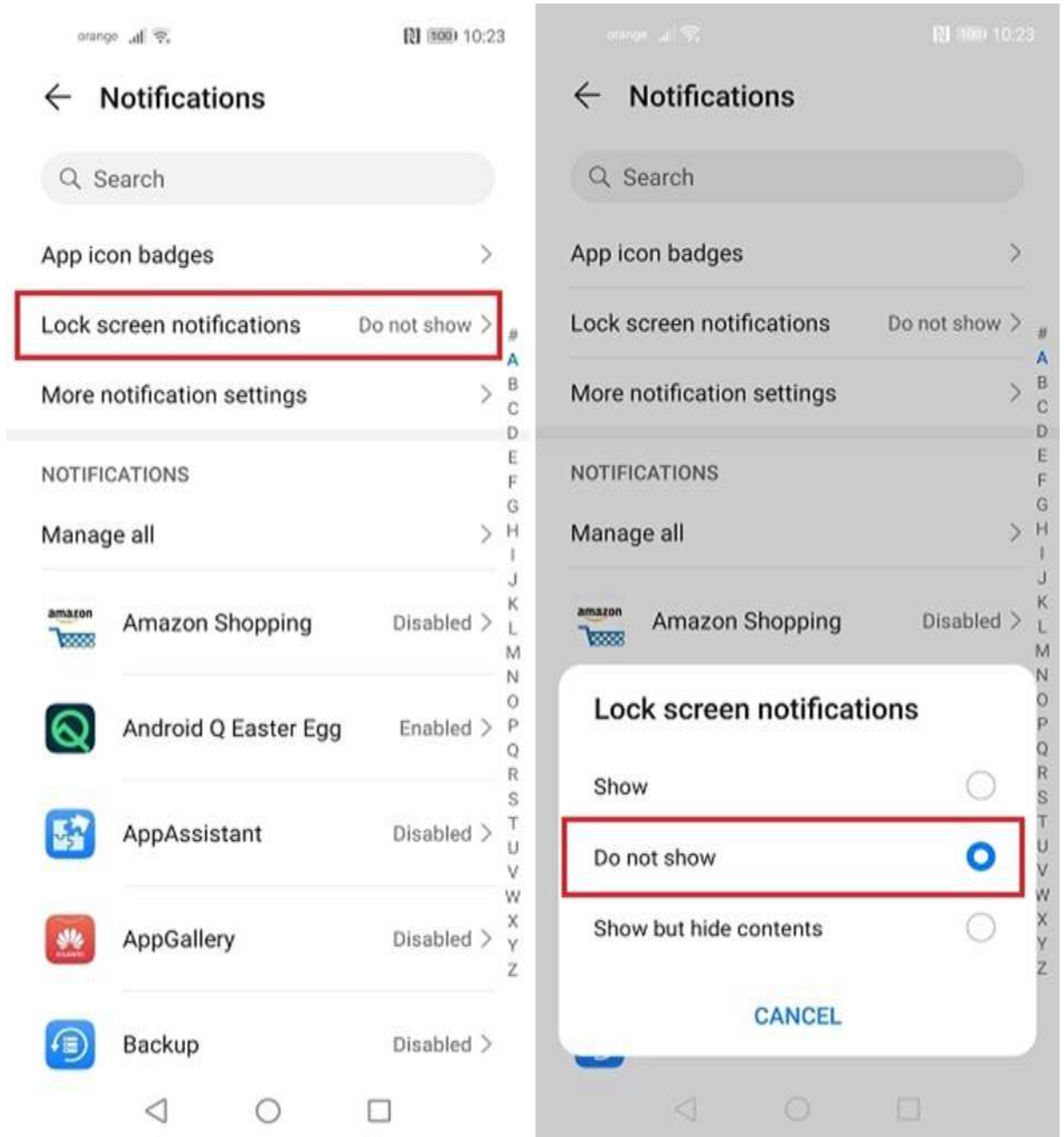
- Settings – Apps & notifications – Advanced – Default apps – Opening links

  Instant apps OFF



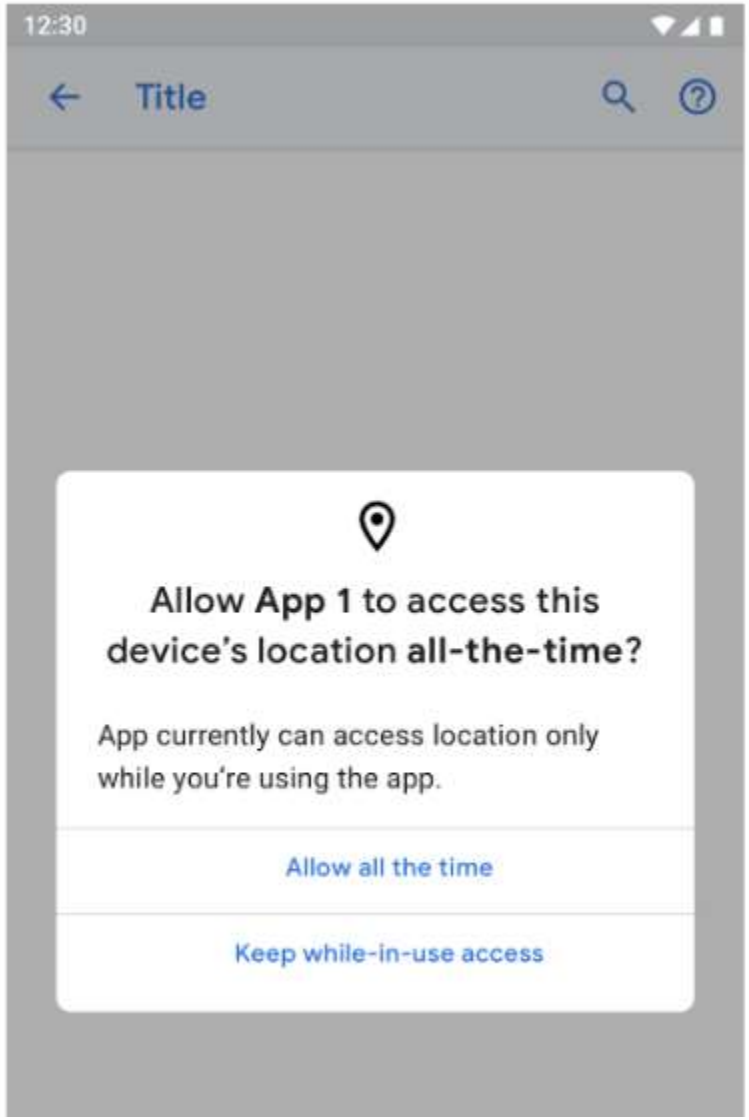
Don’t show notifications as all - Lock screen

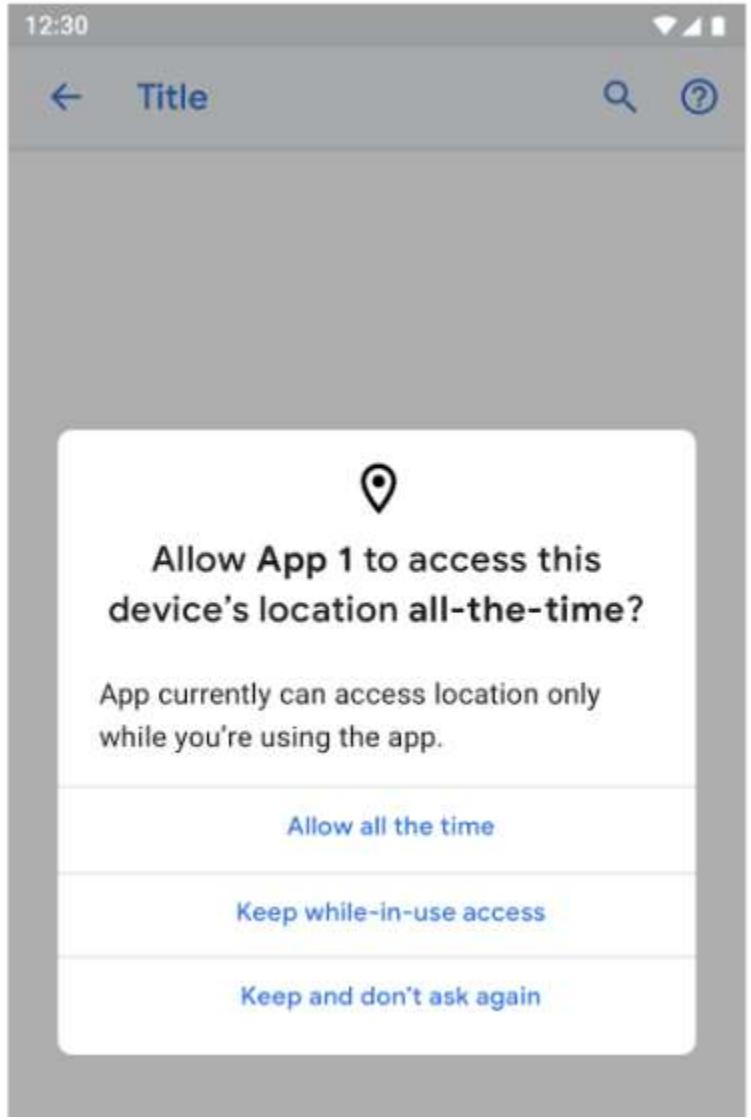
- A REAL privacy issue/setting
- Device unattended, lost, stolen
- Monitor the device notifications for awhile –
- Settings - Apps & notifications – Notifications – Advanced – Lock screen


orange
10:23
Notifications
Search
App icon badges
Lock screen notifications
Do not show
More notification settings
NOTIFICATIONS
Manage all
Amazon Shopping
Disabled
Android Q Easter Egg
Enabled
AppAssistant
Disabled
AppGallery
Disabled
Backup
Disabled
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Lock screen notifications
Show
Do not show
Show but hide contents
CANCEL

‘Use location’ set to ‘Disabled

- Selective
- Some apps worthless without location data
- Some apps malicious use of location data
- Location – cellular data, local Wi-Fi networks, Bluetooth, and GPS
- Location needed for lost device
- Maps – needed
- Facebook - ???

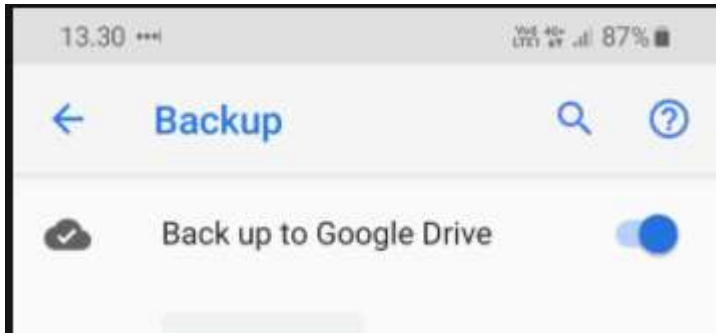

12:30
Title
Allow App 1 to access this device's location all-the-time?
App currently can access location only while you're using the app.
Allow all the time
Keep while-in-use access


12:30
Title
Allow App 1 to access this device's location all-the-time?
App currently can access location only while you're using the app.
Allow all the time
Keep while-in-use access
Keep and don't ask again

Backup to Google Drive

- Personal data: text messages, emails, photos, contacts, etc.
- Helpful – data is backed up off device
- Harmful – Identity thieves can gain access

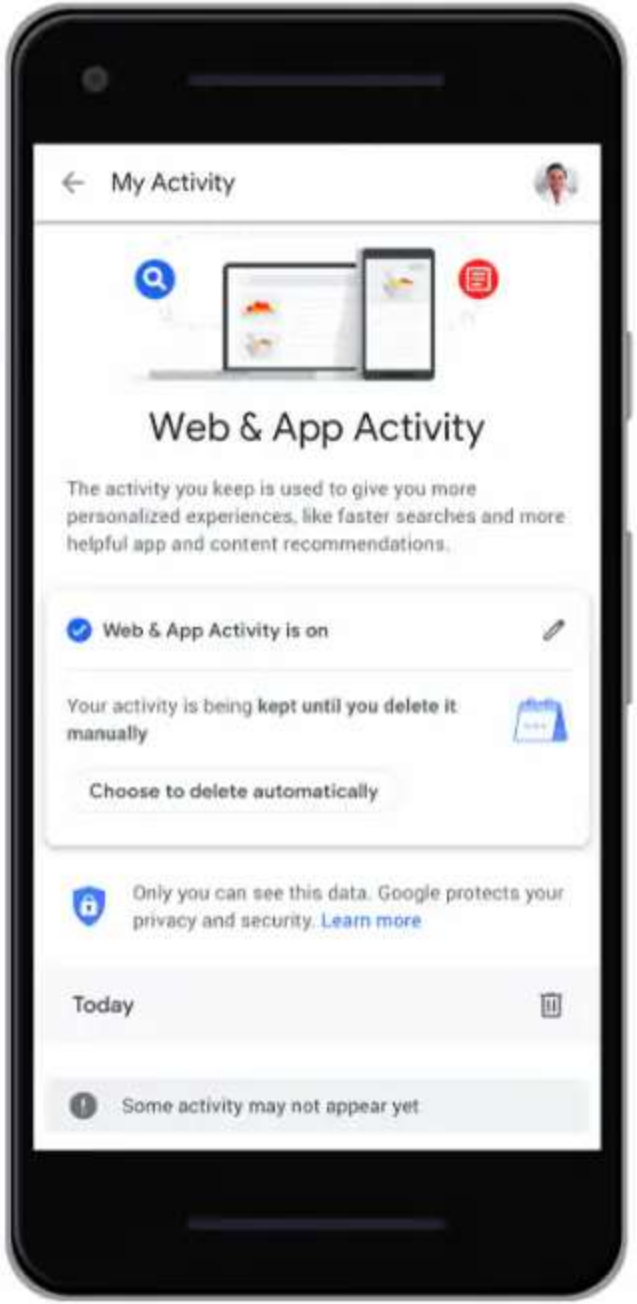
  Your IDentity can be spoofed
- Need to use a Google account associated with the device
- Other services that allow encryption, then backup
- Encryption at backup provider => privacy issues

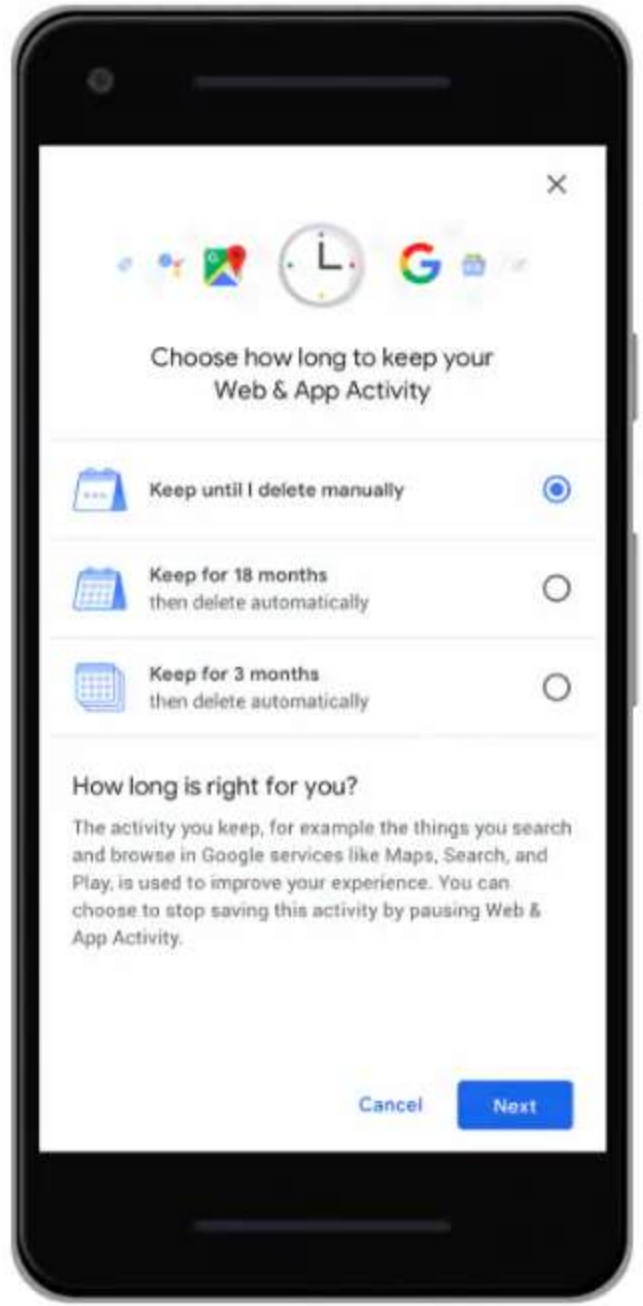


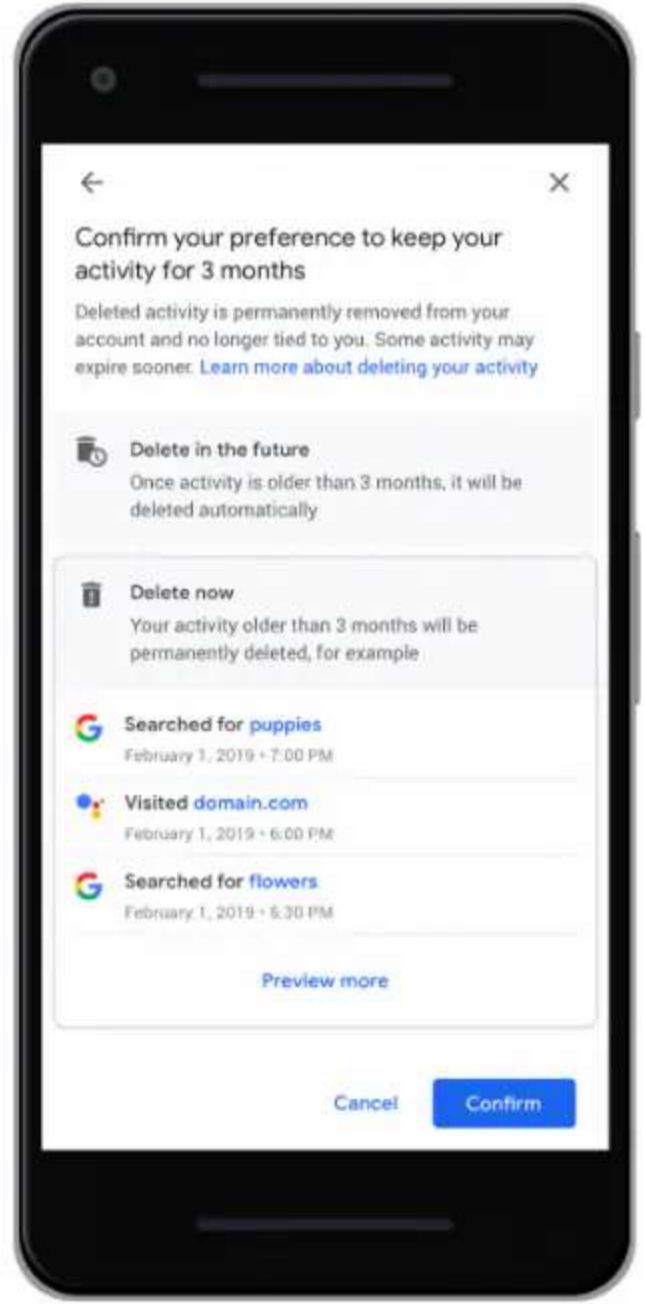
‘Web and App Activity’ set to ‘Disabled’

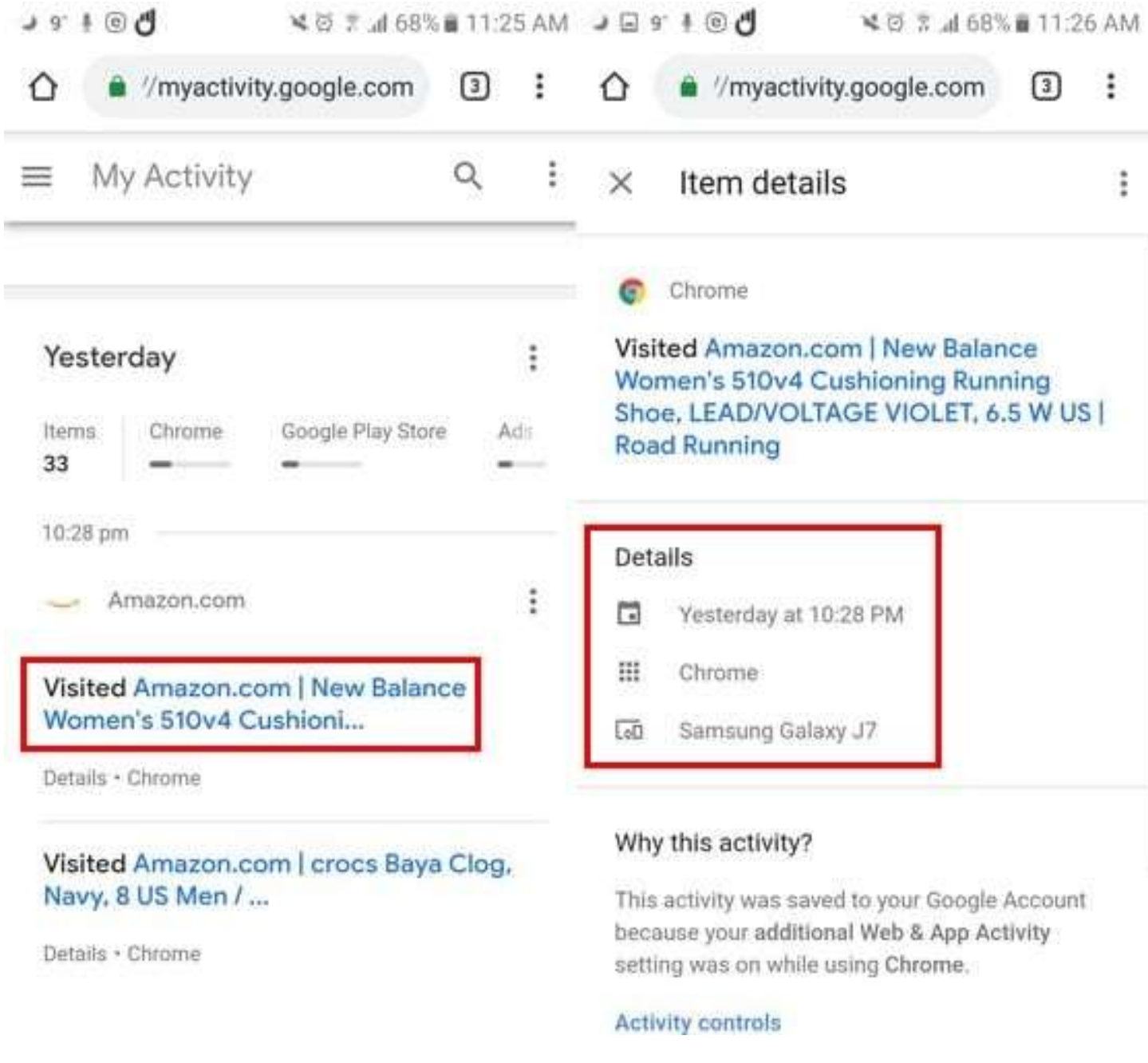
- Pixel devices
- Searches and Activity from other Google services linked and saved to your Google account associated with the device

  even when out are logged out or offline
- Helpful
- Harmful


My Activity
Web & App Activity
The activity you keep is used to give you more personalized experiences, like faster searches and more helpful app and content recommendations.
Web & App Activity is on
Your activity is being kept until you delete it manually
Choose to delete automatically
Only you can see this data. Google protects your privacy and security. Learn more
Today
Some activity may not appear yet

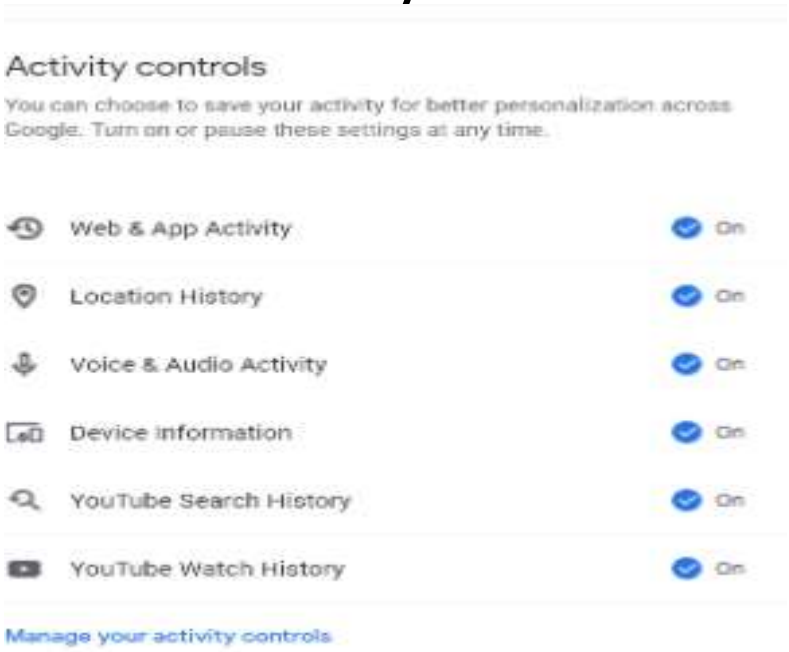

Choose how long to keep your Web & App Activity
Keep until I delete manually
Keep for 18 months
then delete automatically
Keep for 3 months
then delete automatically
How long is right for you?
The activity you keep, for example the things you search and browse in Google services like Maps, Search, and Play, is used to improve your experience. You can choose to stop saving this activity by pausing Web & App Activity.
Cancel
Next


Confirm your preference to keep your activity for 3 months
Deleted activity is permanently removed from your account and no longer tied to you. Some activity may expire sooner. Learn more about deleting your activity
Delete in the future
Once activity is older than 3 months, it will be deleted automatically
Delete now
Your activity older than 3 months will be permanently deleted, for example
Searched for puppies
February 1, 2019 • 7:00 PM
Visited domain.com
February 1, 2019 • 6:00 PM
Searched for flowers
February 1, 2019 • 5:30 PM
Preview more
Cancel
Confirm


68% 11:25 AM
//myactivity.google.com
My Activity
Yesterday
Items
33
Chrome
Google Play Store
10:28 pm
Amazon.com
Visited Amazon.com | New Balance Women's 510v4 Cushioni...
Details • Chrome
Visited Amazon.com | crocs Baya Clog, Navy, 8 US Men / ...
Details • Chrome
68% 11:26 AM
//myactivity.google.com
Item details
Chrome
Visited Amazon.com | New Balance Women's 510v4 Cushioning Running Shoe, LEAD/VOLTAGE VIOLET, 6.5 W US | Road Running
Details
Yesterday at 10:28 PM
Chrome
Samsung Galaxy J7
Why this activity?
This activity was saved to your Google Account because your additional Web & App Activity setting was on while using Chrome.
Activity controls

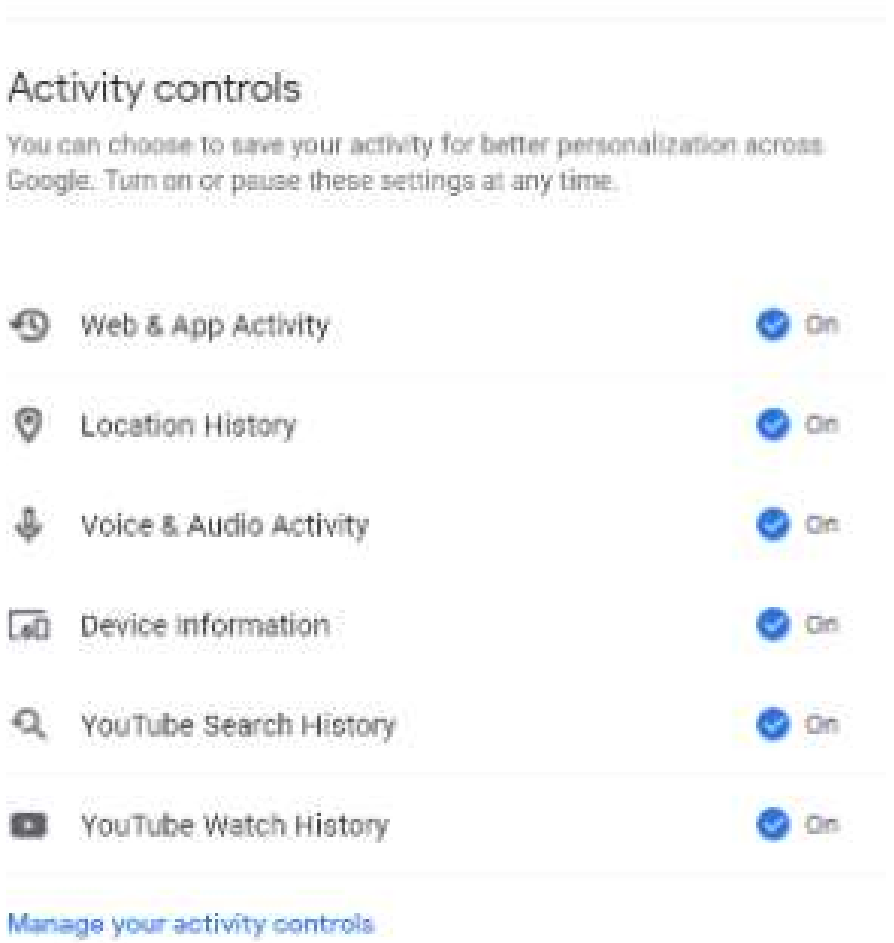
‘Device information’ set to ‘Disabled’

- Personalized information
- PLUS
- Screen on?, Alarms, App lists, battery level, Wi-Fi info, sensor data, …
- Settings – Privacy – Advanced – Activity Controls – Device information



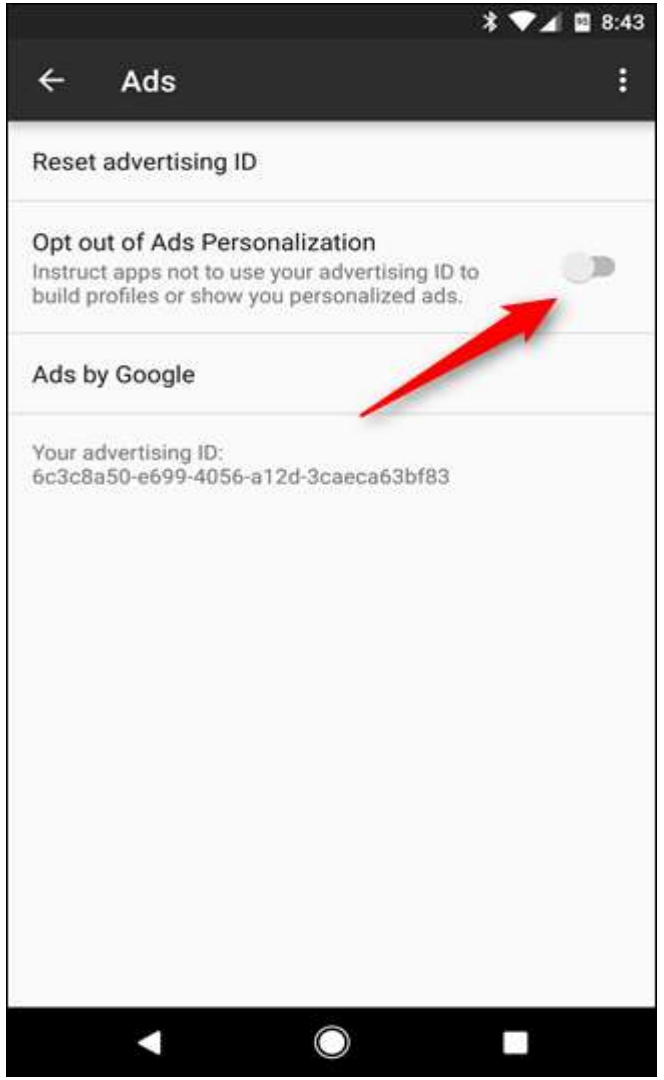
‘Voice and Audio Activity’ ‘ Disabled’

- Voice and *other* audio saved – even while offline
- When setting OFF – stored using anonymous identifiers



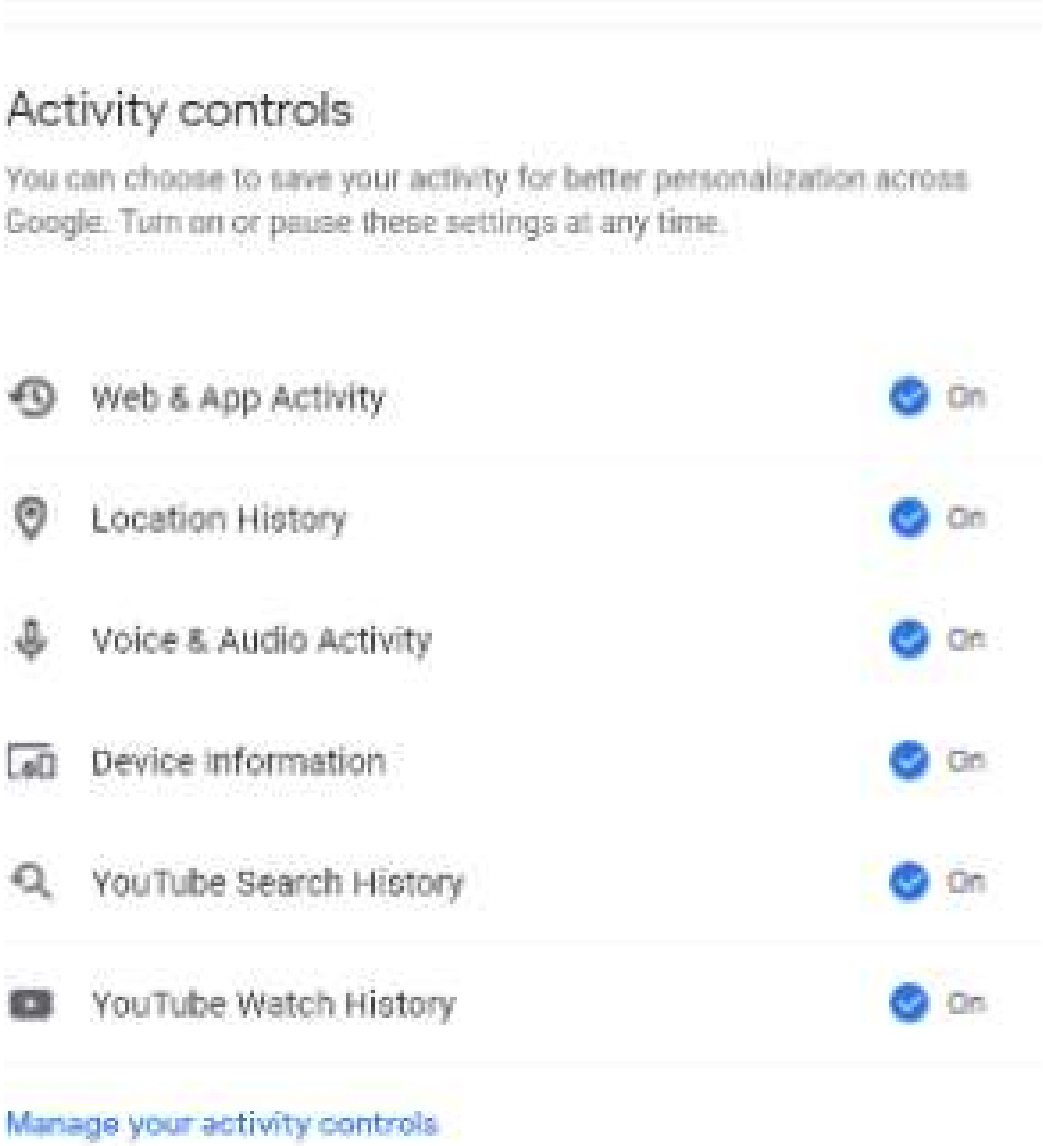
‘Opt out of Ads Personalization’ ON

- Settings – Google – Services – Ads
- Disables profile building



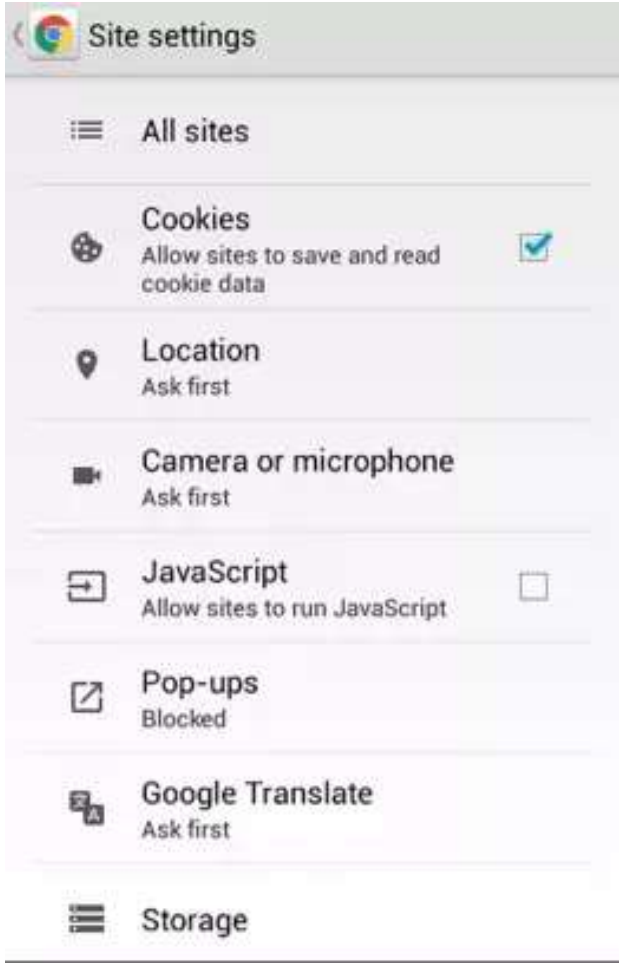
YouTube settings

- Helpful – recommendations
- Harmful –

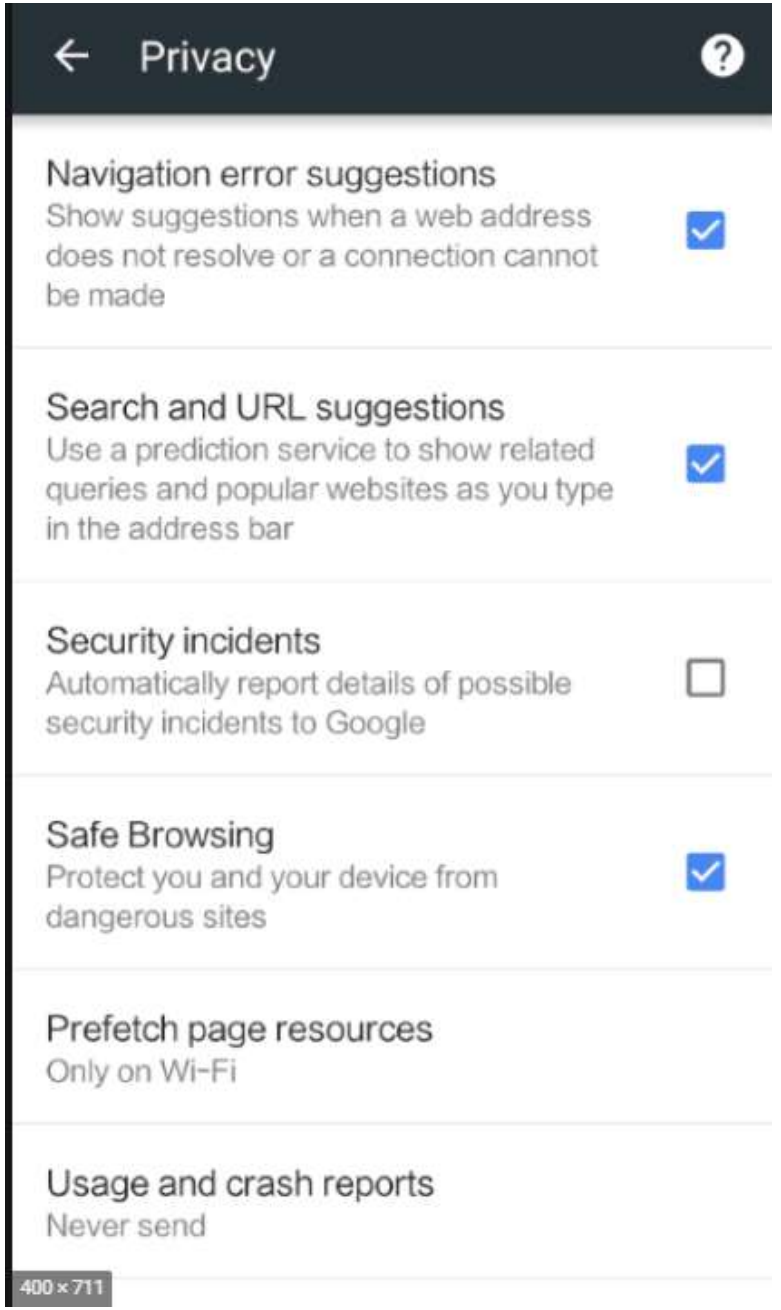


Chrome permissions

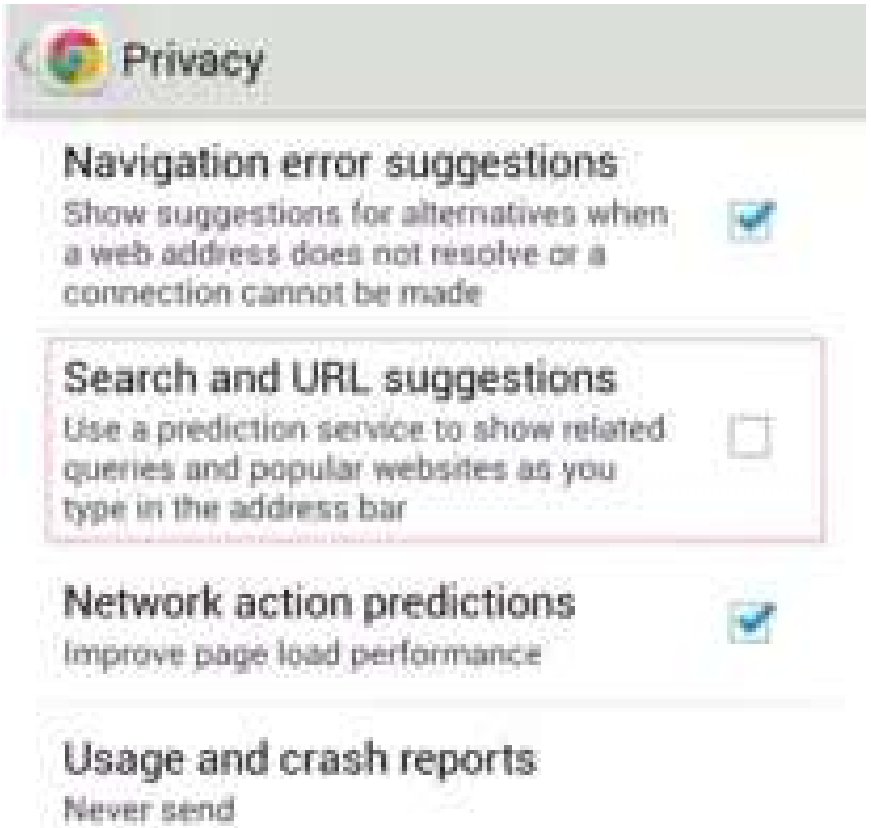
- Chrome – Menu – Settings – Advanced – Site settings – Microphone Ask



Google safe browsing

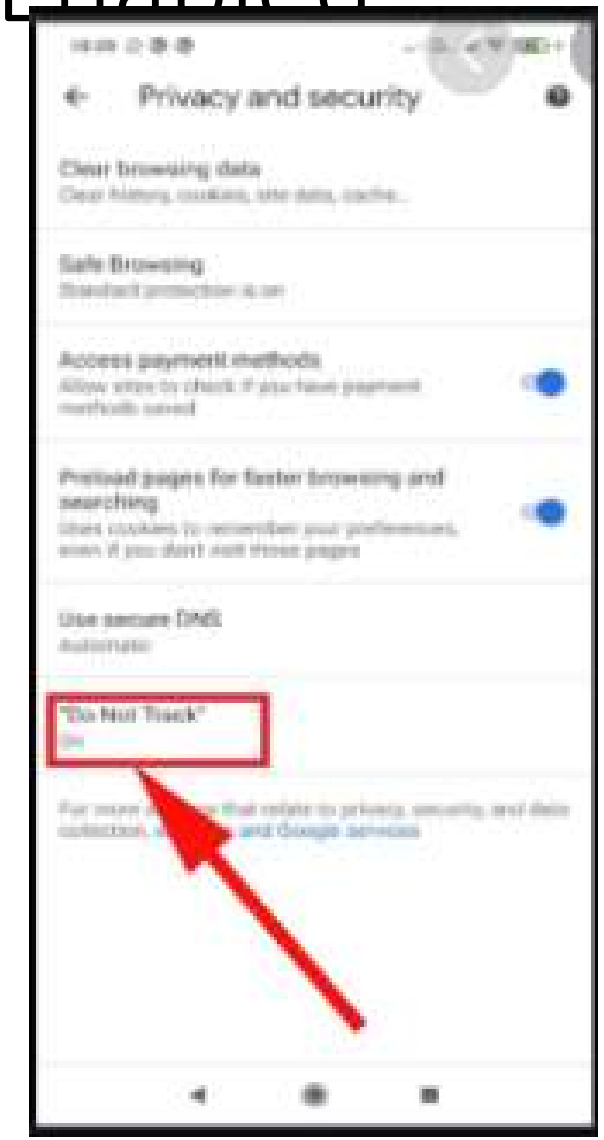


Chrome ‘Search and URL suggestions’ ‘disabled’



Chrome ‘Do Not Track’ ‘ Enabled’

- May or May not limit all WEB sites



The End