Smartphone Snatch Theft

How Smartphone Snatch Theft Happens

Common scenarios

- theft while walking, in crowded areas, or at traffic stops

Methods used by thieves

- quick grabs, distraction techniques

Shoulder hanging

- To grab pin code /pin swipe pattern

Consequences of Smartphone Snatch Theft

Financial impact

- replacement costs, potential data loss

Personal security risks

- loss of sensitive information, identity theft

Emotional toll

- feeling of violation, stress

How to Recover from a Smartphone Theft:1

Immediately Take Action:

- Use a friend's phone or another device to access "Find My iPhone" or "Find My Device" for Android.

- Attempt to remotely lock your phone to prevent unauthorized access.

- If possible, remotely erase your phone to protect sensitive data.

How to Recover from a Smartphone Theft:2

Contact Service Provider:

- Inform your carrier to suspend service to prevent unauthorized calls, texts, and data usage.

- Request a new SIM card if needed for a replacement phone.

Report to Local Authorities:

- File a police report with detailed information about the theft (time, location, device details).

- Share the IMEI number of the phone if possible, which can help authorities track it.

How to Recover from a Smartphone Theft:3

Change Passwords and Secure Accounts:

Immediately change passwords for key accounts linked to the phone, such as email, banking, and social media.

Monitor for unusual activity on any linked accounts and enable two-factor authentication if not already active.

Preventing Smartphone Snatch Theft

Be	Be Aware of Your Surroundings:
Avoid	Avoid using your phone in crowded or public places where it can be easily snatched.
Keep	When walking or commuting, keep your phone in a secure pocket rather than in your hand.
Minimize	Minimize Risk in Vulnerable Situations:
Avoid	Avoid standing near the edge of sidewalks or too close to open vehicle windows when using your phone.
Be	Be cautious when using your phone in places like cafes, public transport, or tourist spots.

Preventing Smartphone Snatch Theft

Physical Security Measures:

Consider using a wrist strap, lanyard, or anti-theft phone case that makes snatching difficult.

Store your phone in a secure bag or inner pocket that is less accessible to potential thieves.

Keeping Backups and Data Security

Set Up	Set Up Regular Backups:
Enable	For iOS: Enable iCloud backups or connect to a computer for local backups via iTunes.
Use	For Android: Use Google Drive to back up data regularly or explore manufacturer-specific backup options.

Keeping Backups and Data Security

Data Encryption and Secure Locking:

- Enable full-disk encryption on your device for added security.

- Use a strong PIN, password, or biometric lock

  - (fingerprint/face ID) to secure the phone.

Keeping Backups and Data Security

Use Security Apps and Settings:

- Install security apps like Lookout or Prey that offer device tracking,

  - remote locking, and wiping capabilities.

- **Familiarize yourself with built-in anti-theft features,**

  - such as Google's Find My Device or Apple's Find My iPhone.

Additional Preventative Measures

Consider Smartphone Insurance:

Look into device insurance policies that cover theft and damage.

Review coverage details to understand what is included and the claims process.

Additional Preventative Measures

Install Anti-Theft Apps:

↓

Consider apps that allow you to remotely lock, locate, or wipe your device if it's stolen.

↓

Apps like Cerberus and Prey offer features beyond what's built into the operating system.

Additional Preventative Measures

Stay Informed and Report Suspicious Activity:

- Join local or online community groups to stay informed about recent theft trends in your area.

- Report suspicious activity to authorities or neighborhood groups to increase awareness.
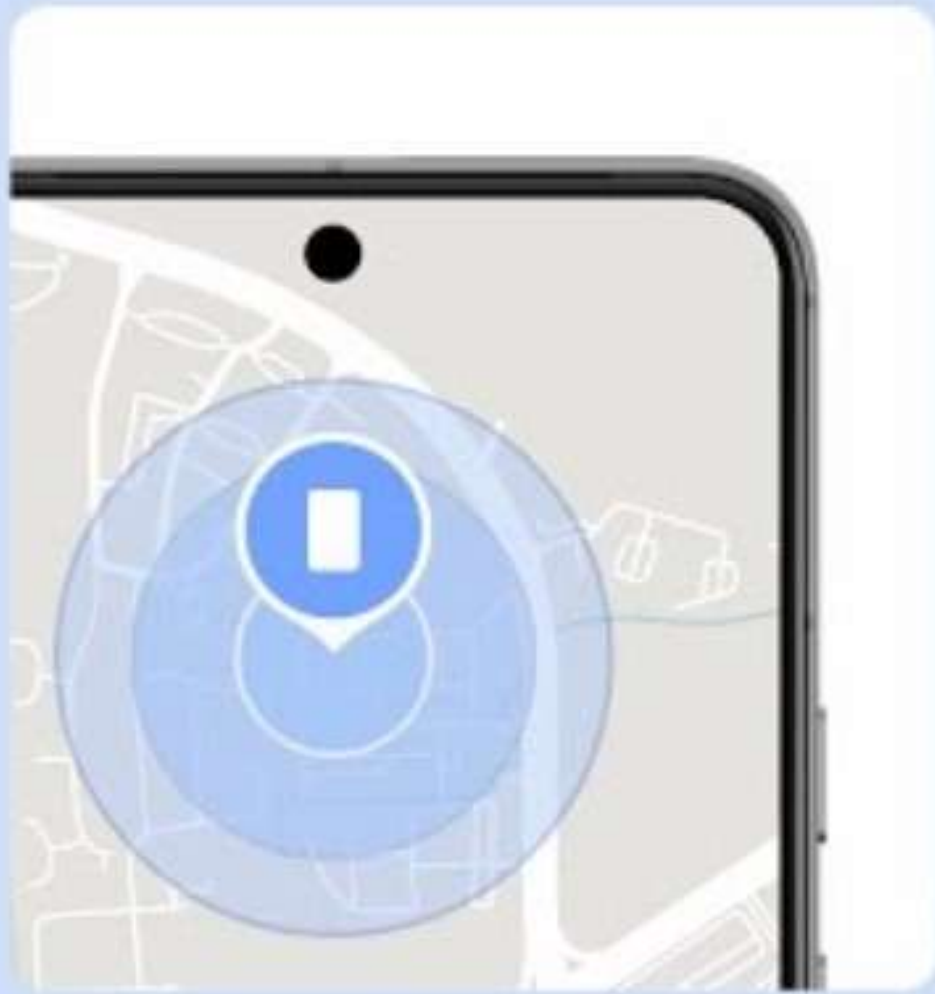
Find My Device

Be ready to find a lost Android device

You can set up Find My Device so you're prepared if you lose your phone, tablet, Wear OS watch, headphones, or something that has a tracker tag attached.

If your device is already lost, learn how to find, secure, or erase it.

Important: Some of these steps work only on Android 9.0 and up. Learn how to check your Android version.

Make sure your device can be found

Step 1: Check that you're signed in to a Google Account   ⌄

Step 2: Check that Location is on   ⌄

Step 3: Check that Find My Device is on   ⌄

Step 4: Find offline devices and devices without power   ⌄

Step 5: Check if your device is listed on Google Play   ⌄

Help

📄 What is a Google Account?

📄 How do I create a new Google Account?

📄 Create a strong password & a more secure account

📄 Verify your account

📄 Control what others see about you across Google services

📄 Someone changed your password

📄 **Be ready to find a lost Android device**

📄 Manage your Location History

📄 Set up a recovery phone number or email address

📄 Turn cookies on or off

📄 How to recover your Google Gmail

Help guide

If your device is already lost, learn how to find, secure, or erase it.

Important: Some of these steps work only on Android 9.0 and up. Learn how to check your Android version.

Make sure your device can be found

Step 1: Check that you're signed in to a Google Account   ⌄

Step 2: Check that Location is on   ⌄

Step 3: Check that Find My Device is on   ⌄

Step 4: Find offline devices and devices without power   ⌄

Step 5: Check if your device is listed on Google Play   ⌄

Step 6: Check that you can find your device   ⌄

Step 7: Install the Find My Device app   ⌄

Step 8: Create a 2-Step Verification backup code   ⌄

Add headphones or other accessories

⊙ Help guide

My Devices

Redmi Note 9

Galaxy S8

OnePlus 6

Galaxy S10

Galaxy S7

Lenovo Tab M10 Plus 3rd

← ⛶   ⚙   ↻
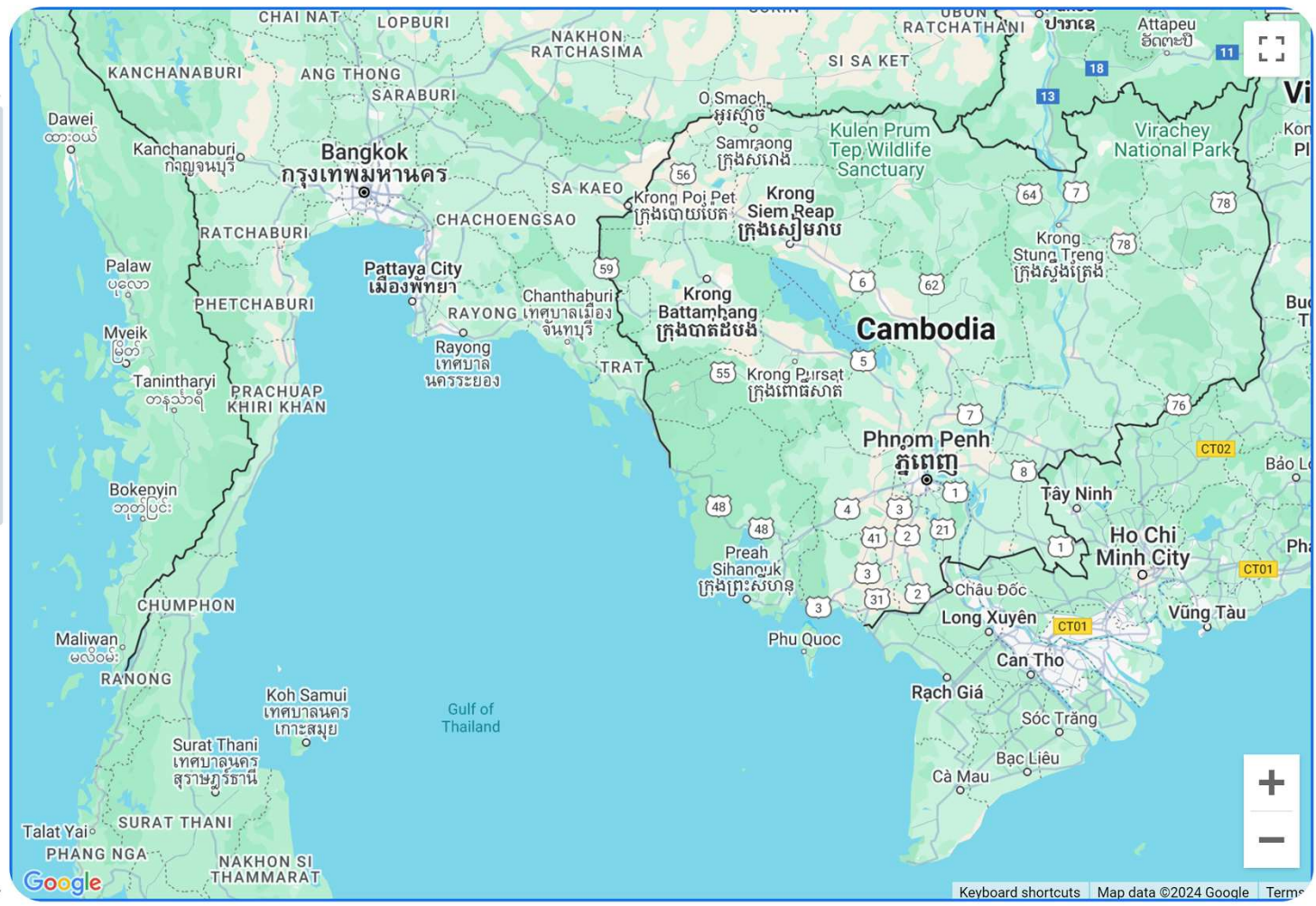
Galaxy S8
Last seen just now
▼ ITN3BB_5GHz 🔋 21%

ᵢₗ Play sound
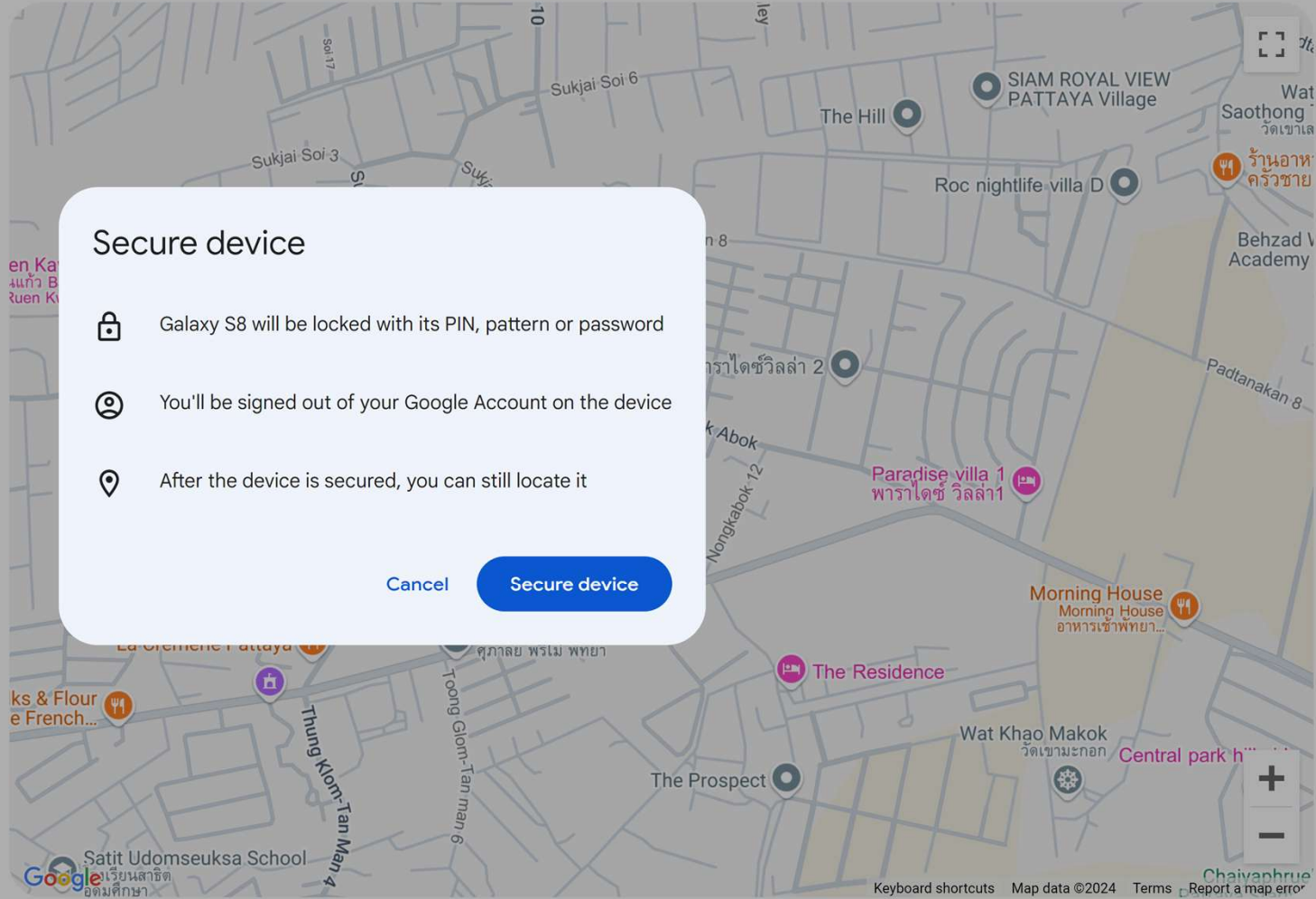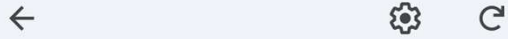
🔒 Secure device

📱✕ Factory reset device

Secure device

🔒 Galaxy S8 will be locked with its PIN, pattern or password

👤 You'll be signed out of your Google Account on the device

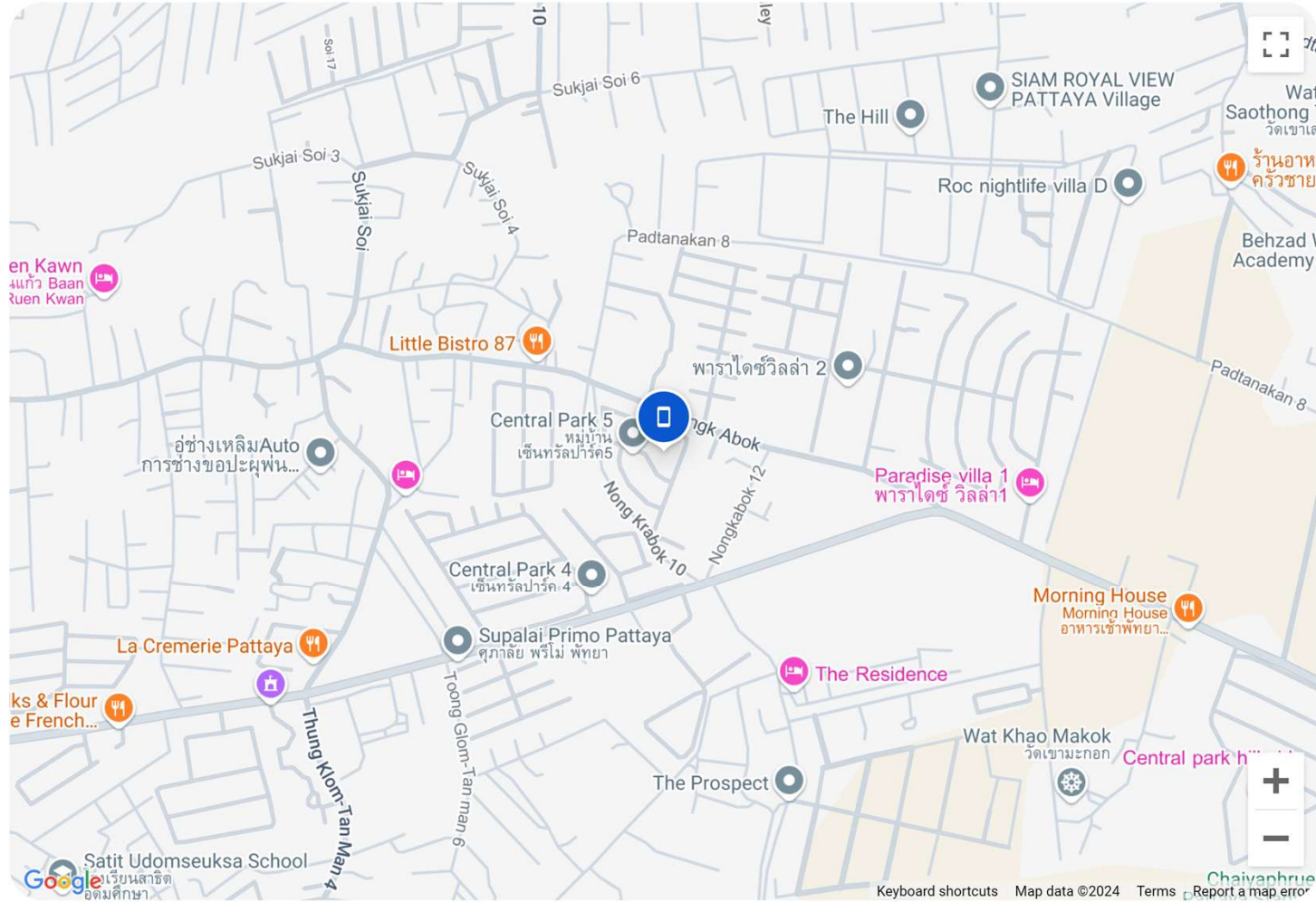📍 After the device is secured, you can still locate it

Cancel   **Secure device**

Remote Lock

Google Pixel 6a

Last seen 4 minutes ago

ITN3BB_2.4GHz 78%

Play sound

Secure device

Factory reset device

SIAM ROYAL VIEW
PATTAYA Village

Wat
Saothong

The Hill

ร้านอาห
ครัวชาย

Roc nightlife villa D

Behzad V
Academy

Sukjai Soi 6

Sukjai Soi 3

Sukjai Soi

Padtanakan 8

Padtanakan 8

en Kawn
แก้ว Baan
Ruen Kwan

Little Bistro 87

พาราไดซ์วิลล่า 2

Central Park 5
หมู่บ้าน
เซ็นทรัลปาร์ค5

Paradise villa 1
พาราไดซ์ วิลล่า1

อู่ช่างเหลิมAuto
การช่างขอปะผุผพน...

gk Abok

Nong Krabok 10

Nongkabok 12

Central Park 4
เซ็นทรัลปาร์ค 4

Morning House
Morning House
อาหารเช้าพัทยา...

La Cremerie Pattaya

Supalai Primo Pattaya
ศุภาลัย พรีโม่ พัทยา

The Residence

ks & Flour
e French...

Wat Khao Makok
วัดเขามะกอก

Central park h

The Prospect

Satit Udomseuksa School
โรงเรียนสาธิต
อุดมศึกษา

Chaiyaphrue

Use Find My

The Annoying Problem with "Prey"

- You have to give full access to Prey
- This means it's always running in the background over other apps
- So your banking apps won't work until you turn accessibility off for Prey
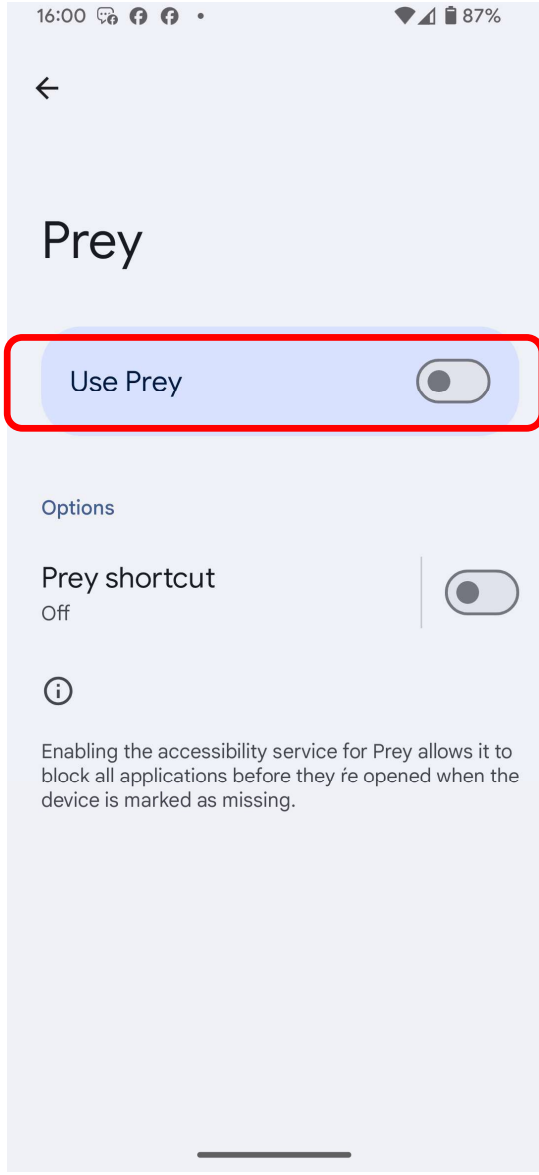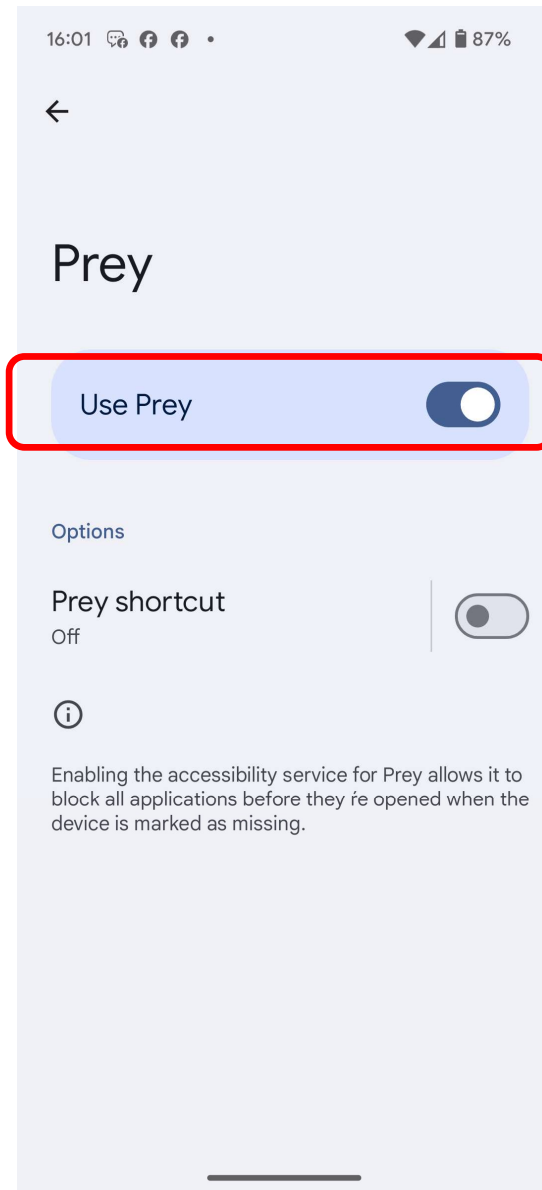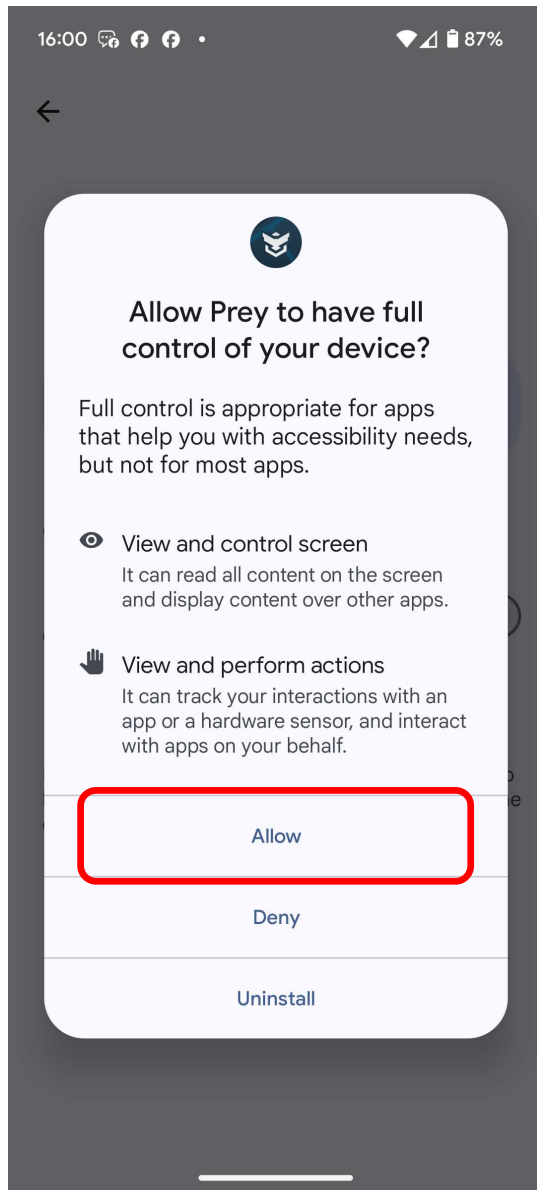
Keep a Screen Shot of your IMEI Number

- Go to "settings"
- Then "About phone"
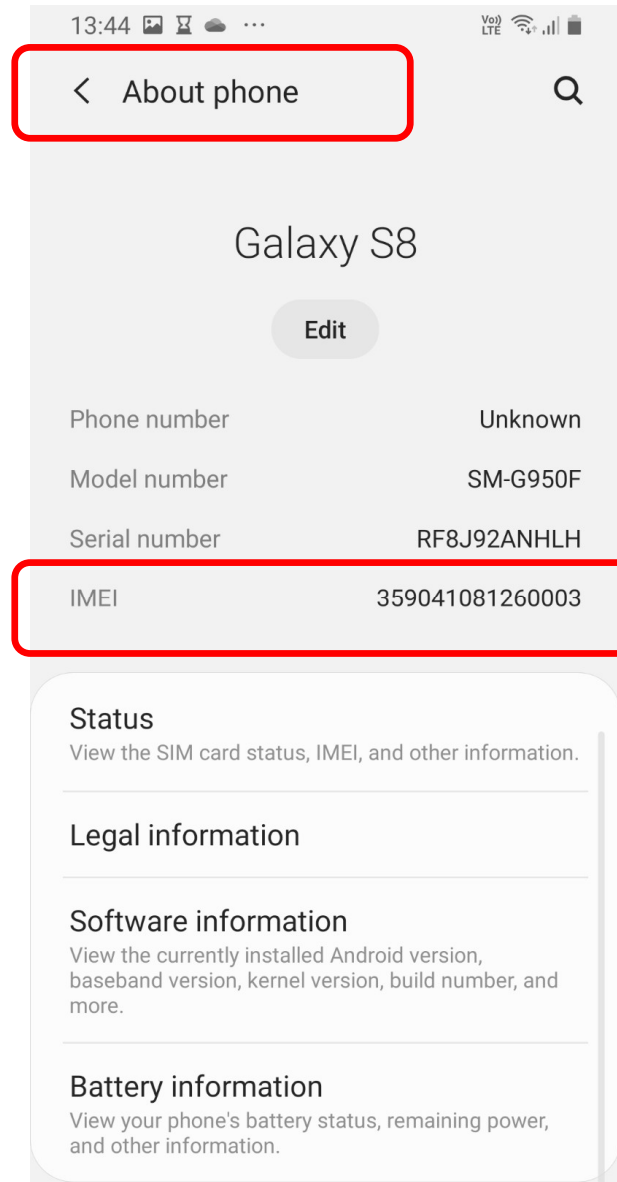
Put a PIN Code on your SIM card

You will need this to avoid the thief using your phone....

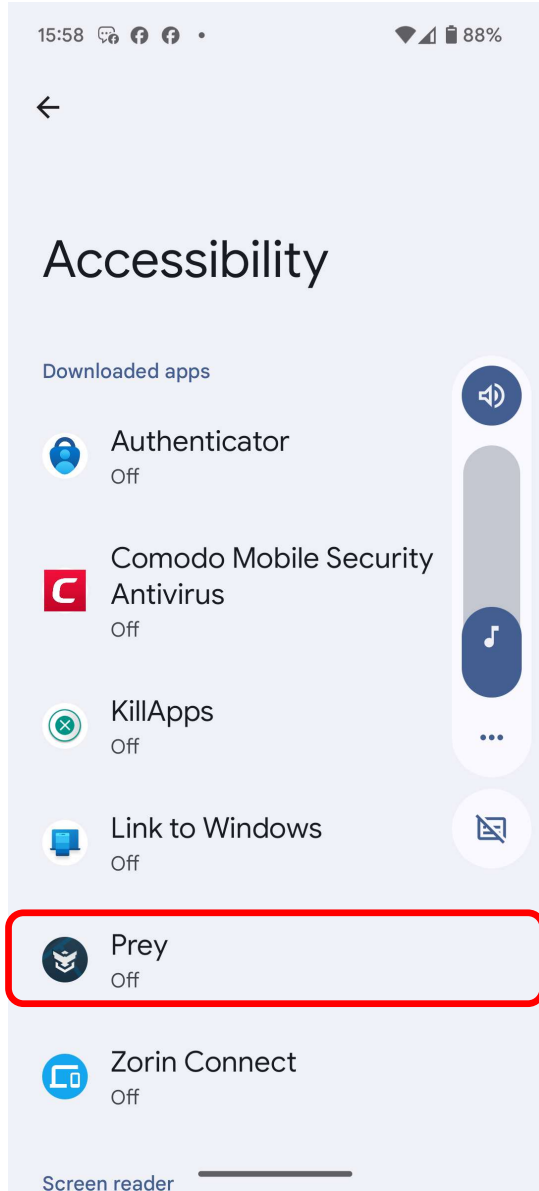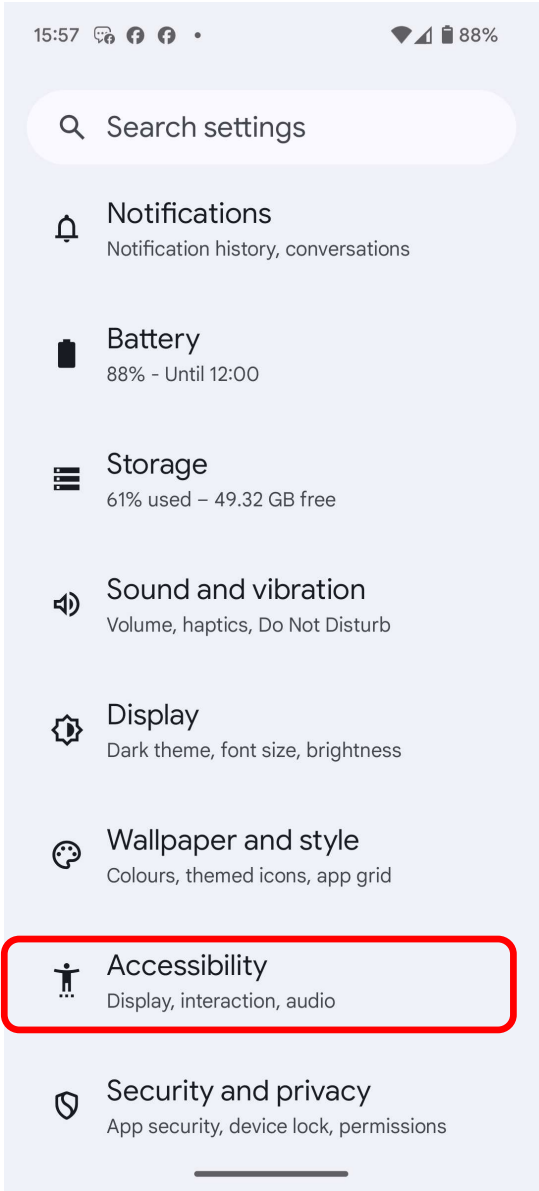- <mark>BUT FIRST GET YOUR PHONE'S "PUK" CODE (Personal Unlock Key)</mark>

- If you have the original card the SIM card came with the PUK is there.

- If not call your phone service provider & ask for it

- E.g. for DTAC call 1678 the 4 to talk to rep

- The PUK code is 8 digits, do not lose it!
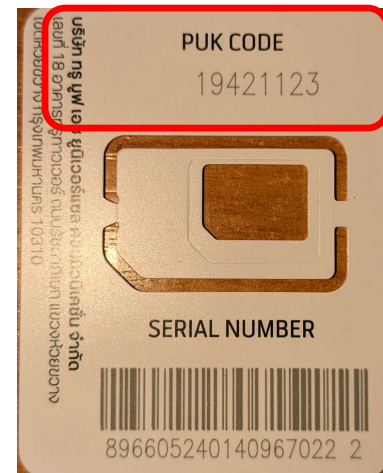
Put a lock on your Sim Card

Screen 1 — Settings

Wallpapers and themes
Wallpapers, Themes, Icons

Lock screen
Screen lock type, Always On Display, Clock style

Biometrics and security
Face recognition, Iris, Privacy

Accounts and backup
Samsung Cloud, Smart Switch

Google
Google settings

Advanced features
Motions and gestures, One-handed mode

Device care
Battery, Storage, Memory, Security

Apps
Default apps, App permissions

Screen 2 — Biometrics and security

13:46

← Biometrics and security

Secure Folder
Keep your personal files and apps safe and secure.

Secure startup
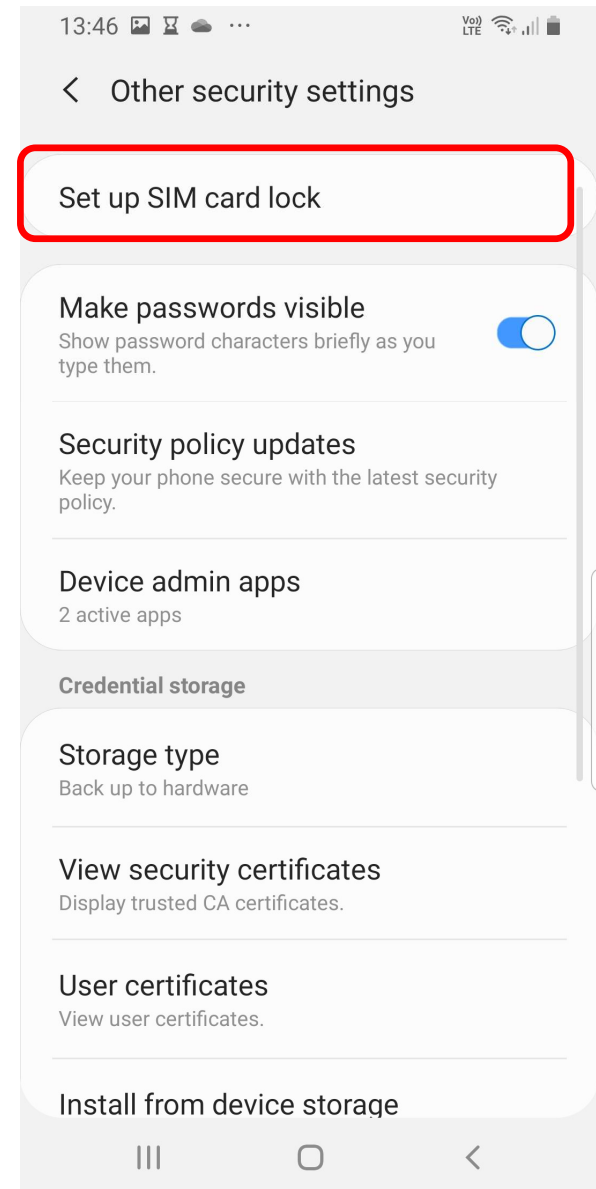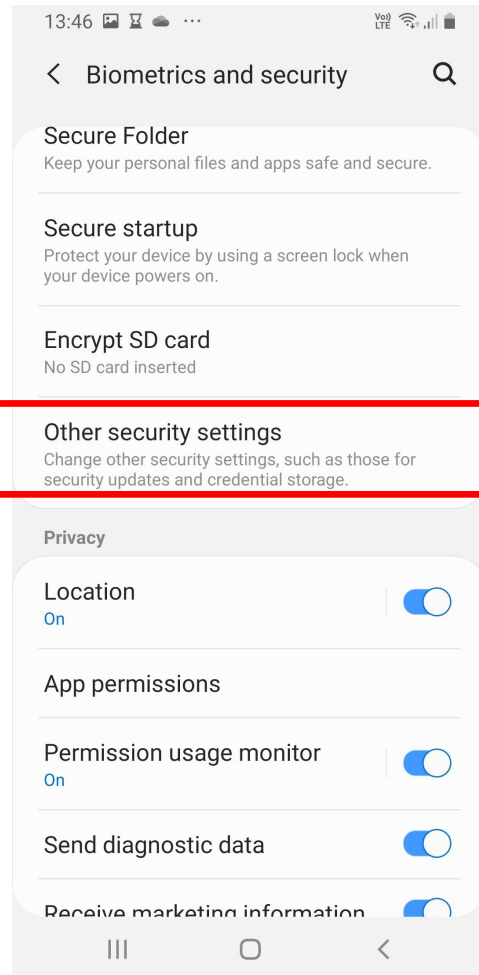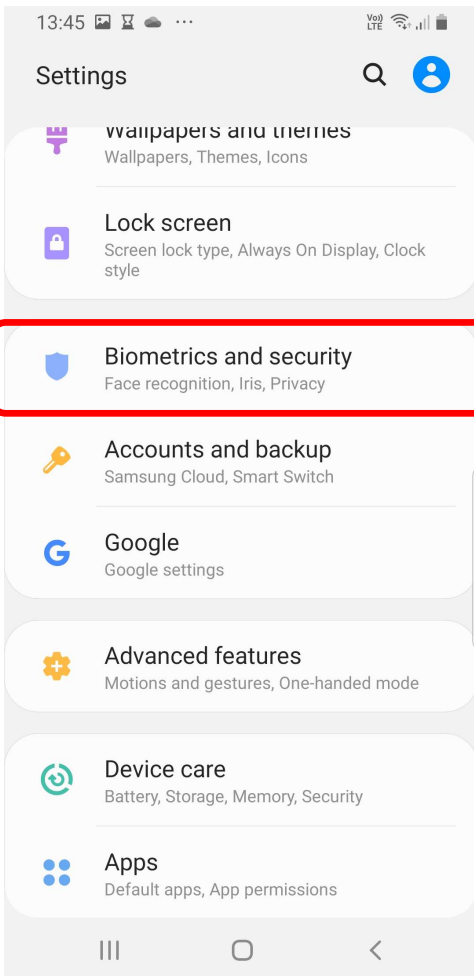Protect your device by using a screen lock when your device powers on.

Encrypt SD card
No SD card inserted

Other security settings
Change other security settings, such as those for security updates and credential storage.

Privacy

Location
On

App permissions

Permission usage monitor
On

Send diagnostic data

Receive marketing information

Screen 3 — Other security settings

13:46

← Other security settings

Set up SIM card lock

Make passwords visible
Show password characters briefly as you type them.

Security policy updates
Keep your phone secure with the latest security policy.

Device admin apps
2 active apps

Credential storage

Storage type
Back up to hardware

View security certificates
Display trusted CA certificates.

User certificates
View user certificates.

Install from device storage