Android - Security features to reduce the chance of stolen data

WHY DO YOU NEED TO MAKE YOUR ANDROID PHONE MORE SECURE?

Android is a mobile operating system developed and released by Google for use in a variety of hand-held devices, such as smart phones, tablets and wearables.

Your phones security is maintained through the combination of your Biometric (Face & Fingerprint), phone passcode and Google account. If your phone is left unlocked or stolen, a lot of personal and dangerous information can be available to anyone and is valuable to fraudsters, hackers and data brokers.

Here are some of the harmful things that can be done to you:

- Change the Android passcode / biometric settings
- Turn off two-factor authentication.
- Disable Find My Device.
- Lock you out of other devices signed in with the same Google ID.
- Access personal information stored in your google account and other apps on your phone:
    - Social media accounts (Facebook, X, TikTok, Instagram, SnapChat…)
    - Email accounts (Gmail, Outlook…)
    - Shopping platform accounts (Amazon, Vinted, eBay, Tesco...)
- Access financial, pass and ticket information stored in your Google Wallet:
    - Bank Account / Card details
    - Membership and Loyalty card accounts
    - Train tickets and Boarding passes

Even without knowledge of your passcode, if a phone is stolen from out of your hand when unlocked (e.g. when on a call), a thief has access to:

- All your device information, emails, social media, notes and photos etc
- And much, much more…

This guide is based upon Googles Android Operating System (OS), which is found on Pixel devices only. However due to a variety of Original Equipment Manufacturers (OEM)(Samsung, Xiaomi, One Plus etc.) android versions, which are built on Google's open-source Android with custom User Interfaces (UI), some of the features may be named differently, unavailable or in a different settings area on your device.

Please consult your manufacturers device user guide or search your settings on your phone for the phrase shown in the [ ] brackets after every section title.

This guide outlines our recommended settings to keep your device secure, and assumes you are keeping your device up to date on the latest android version, available from your manufacturer.

1. TURN ON ADVANCED PROTECTION [*Advanced Protection*]

Androids Advanced Protection is a one stop shop for a lot of the individual features listed further down in this guide, if your Android OS supports it, it is the single most secure thing you can do after setting a strong passcode.

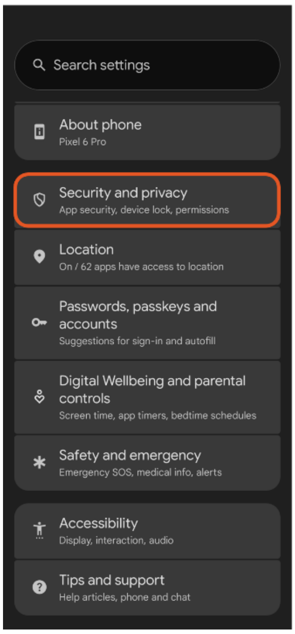
When you turn on Advanced Protection, you get the strongest security and privacy features to protect you and your device against online attacks, harmful apps, and data risks. When enabled these privacy features cannot be turned off individually, some key features include:

- App protection from malware and unknown sources
- Automatic device locking due to Theft Detection and Inactivity
- Identification of Spam, Scam and Unsafe messages and links
- Spam Caller ID and Call Screening
- Enforcement of safe and secure browsing

To enable Advanced Protection:

- Step 1: Open 'Settings' ⚙ (cog icon)
- Step 2: Select 'Security and Privacy'
- Step 3: Scroll down and select 'Advanced Protection'
- Step 4: Slide the 'Device Protection' right to on
- Step 5: A prompt will ask you to confirm 'Turn on'.

2.



Search settings

About phone
Pixel 6 Pro

Security and privacy
App security, device lock, permissions

Location
On / 62 apps have access to location

Passwords, passkeys and accounts
Suggestions for sign-in and autofill

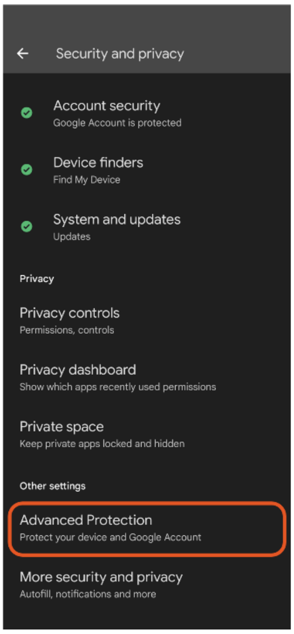
Digital Wellbeing and parental controls
Screen time, app timers, bedtime schedules

Safety and emergency
Emergency SOS, medical info, alerts

Accessibility
Display, interaction, audio

Tips and support
Help articles, phone and chat

3.



Security and privacy

Account security
Google Account is protected

Device finders
Find My Device

System and updates
Updates

Privacy

Privacy controls
Permissions, controls

Privacy dashboard
Show which apps recently used permissions

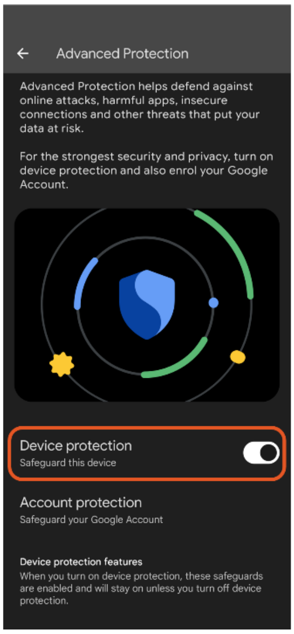
Private space
Keep private apps locked and hidden

Other settings

Advanced Protection
Protect your device and Google Account

More security and privacy
Autofill, notifications and more

4.



Advanced Protection

Advanced Protection helps defend against online attacks, harmful apps, insecure connections and other threats that put your data at risk.

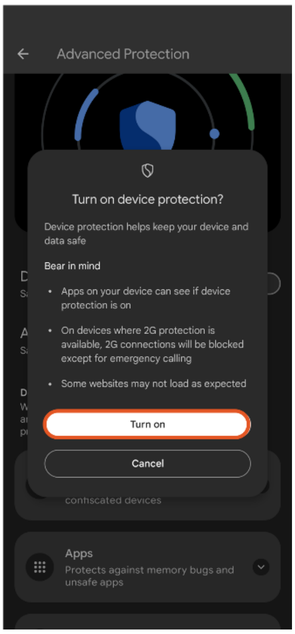
For the strongest security and privacy, turn on device protection and also enrol your Google Account.

Device protection
Safeguard this device

Account protection
Safeguard your Google Account

Device protection features
When you turn on device protection, these safeguards are enabled and will stay on unless you turn off device protection.

5.



Advanced Protection

Turn on device protection?

Device protection helps keep your device and data safe

Bear in mind

- Apps on your device can see if device protection is on
- On devices where 2G protection is available, 2G connections will be blocked except for emergency calling
- Some websites may not load as expected

Turn on

Cancel

confiscated devices

Apps
Protects against memory bugs and unsafe apps

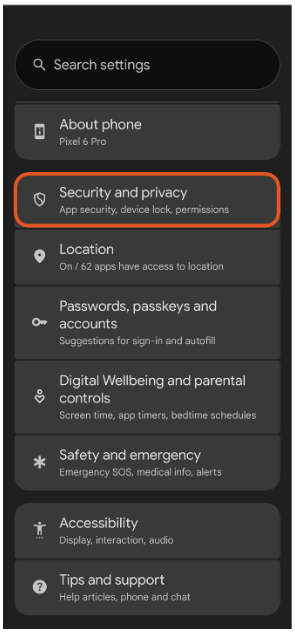
2. ENABLE FIND HUB [*Find My Device*]

Find Hub is an evolution of the find my phone feature, allowing users to not only find their device if stolen, but also locate it along with other accessories when misplaced or lost. The Find Hub also allows families and/or friends to track each other's location, similar to Snapchat's 'Snap Maps'.

To enable Find Hub:

- Step 1: Open 'Settings' ⚙ (cog icon)
- Step 2: Select 'Security and Privacy'
- Step 3: Select 'Device Finders'
- Step 4: Select 'Find Hub'
- Step 5: Slide the 'Allow device to be located' right to on.

2.



Search settings

About phone
Pixel 6 Pro

Security and privacy
App security, device lock, permissions

Location
On / 62 apps have access to location

Passwords, passkeys and accounts
Suggestions for sign-in and autofill

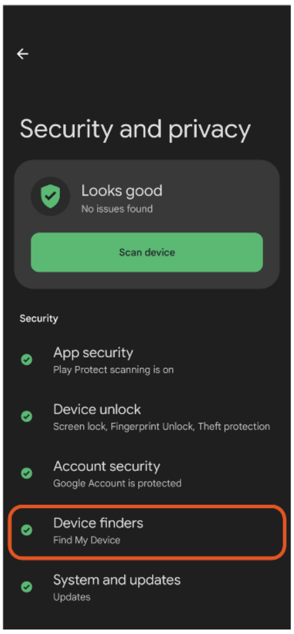
Digital Wellbeing and parental controls
Screen time, app timers, bedtime schedules

Safety and emergency
Emergency SOS, medical info, alerts

Accessibility
Display, interaction, audio

Tips and support
Help articles, phone and chat

3.



Security and privacy

Looks good
No issues found

Scan device

Security

App security
Play Protect scanning is on

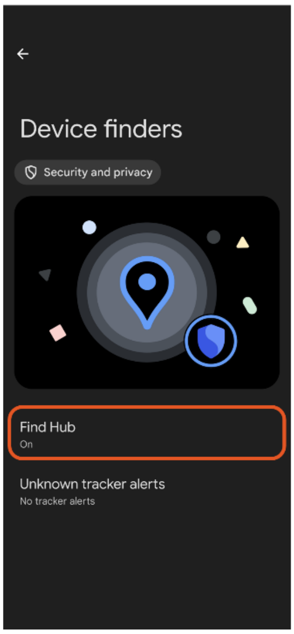
Device unlock
Screen lock, Fingerprint Unlock, Theft protection

Account security
Google Account is protected

Device finders
Find My Device

System and updates
Updates

4.



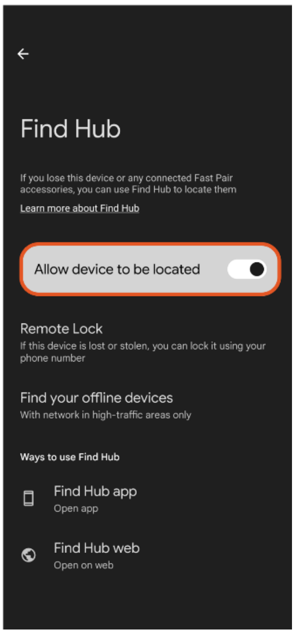
Device finders

Security and privacy

Find Hub
On

Unknown tracker alerts
No tracker alerts

5.



Find Hub

If you lose this device or any connected Fast Pair accessories, you can use Find Hub to locate them

Learn more about Find Hub

Allow device to be located ●

Remote Lock
If this device is lost or stolen, you can lock it using your phone number

Find your offline devices
With network in high-traffic areas only

Ways to use Find Hub

Find Hub app
Open app

Find Hub web
Open on web

Within Find Hub you will also find options to allow you to remotely lock your device if stolen, links to the Find Hub app and website and find your offline device options.

Within device finders, you can enable alerts for 'Unknown Tracker Alerts', this will tell you if a digital tracking tag, that is not yours, is attached to you or in a bag etc.

3. SET AN ALPHANUMERIC PASSCODE [*Screen Lock*]

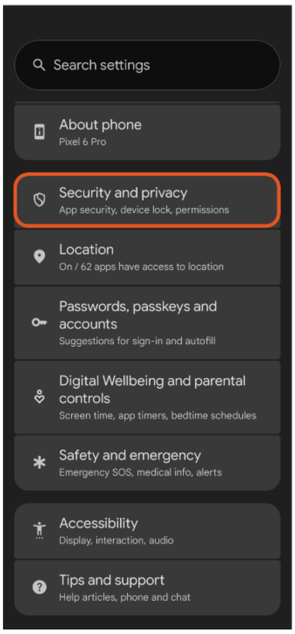
If you are still using a 4-6 digit pin or a pattern on your phone, even if your using a fingerprint or Face Unlock day-to-day, it’s time to upgrade your passphrase, as an easy guessable or observable pin undermines the security of biometrics (fingerprint or face).

Like most passwords today a combination of upper- and lower-case letters and numbers, known as alphanumeric, is more secure than a pin or an all single-case word!

To set an alphanumeric passcode:

- Step 1: Open ‘Settings’ ⚙ (cog icon)
- Step 2: Select ‘Security and Privacy’
- Step 3: Select ’Device Unlock’
- Step 4: Select the ‘Screen lock’ wording and not the cog, you will be prompted for you current pin or pattern
- Step 5: Now choose ‘Password’, you will be prompted to enter a new passphrase twice to confirm.

2.



Search settings

About phone
Pixel 6 Pro

Security and privacy
App security, device lock, permissions

Location
On / 62 apps have access to location

Passwords, passkeys and accounts
Suggestions for sign-in and autofill

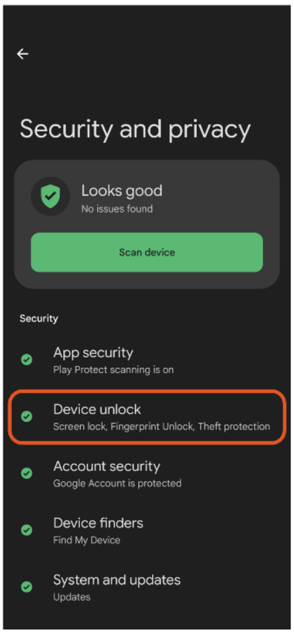
Digital Wellbeing and parental controls
Screen time, app timers, bedtime schedules

Safety and emergency
Emergency SOS, medical info, alerts

Accessibility
Display, interaction, audio

Tips and support
Help articles, phone and chat

3.



Security and privacy

Looks good
No issues found

Scan device

Security

App security
Play Protect scanning is on

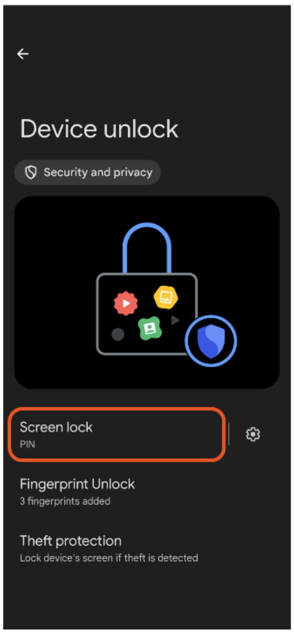
Device unlock
Screen lock, Fingerprint Unlock, Theft protection

Account security
Google Account is protected

Device finders
Find My Device

System and updates
Updates

4.



Device unlock

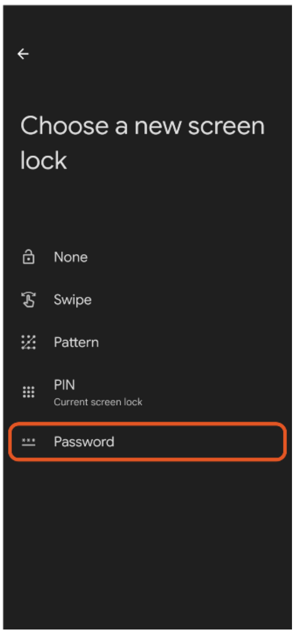
Security and privacy

Screen lock
PIN

Fingerprint Unlock
3 fingerprints added

Theft protection
Lock device's screen if theft is detected

5.



Choose a new screen lock

None

Swipe

Pattern

PIN
Current screen lock

Password

4. AUTOMATIC SCREEN LOCK [*Screen timeout*]

Preventing someone accessing your phone, if you happen to leave it unlocked on a table, we've all done it, you can set the screen locking settings to immediately lock your device when your screen times out.

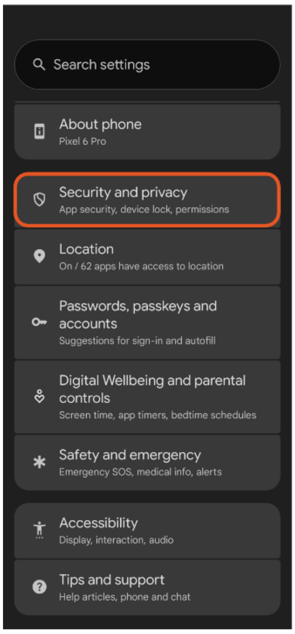
Android lets you choose the time it will take for your device to lock once the screen goes black, anywhere from immediately up to 30 minutes. The longer you leave it the more vulnerable your device and data is, however, you should adjust this timing to suit your needs, acknowledging the risk and in conjunction with the 'Screen timeout' you set in section 7.

A recommended guideline is either 5 seconds, which will allow you to tap your screen just as it goes black, or if unsure start with immediately.

To enable Advanced Protection:

- Step 1: Open 'Settings' ⚙ (cog icon)
- Step 2: Select 'Security and Privacy'
- Step 3: Select 'Device unlock'
- Step 4: Select the 'Screen lock' 'settings cog'.
- Step 5: Select 'Lock after screen timeout' select the shortest period that is suitable for you.

2.



Search settings

About phone
Pixel 6 Pro

Security and privacy
App security, device lock, permissions

Location
On / 62 apps have access to location

Passwords, passkeys and accounts
Suggestions for sign-in and autofill

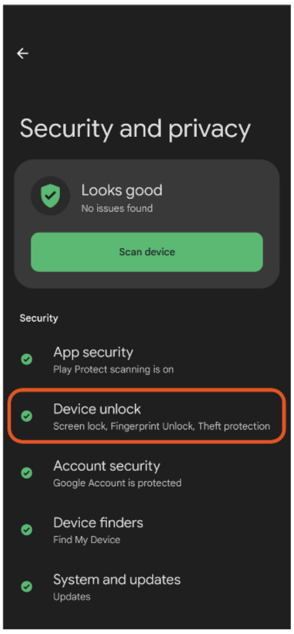
Digital Wellbeing and parental controls
Screen time, app timers, bedtime schedules

Safety and emergency
Emergency SOS, medical info, alerts

Accessibility
Display, interaction, audio

Tips and support
Help articles, phone and chat

3.



Security and privacy

Looks good
No issues found

Scan device

Security

App security
Play Protect scanning is on

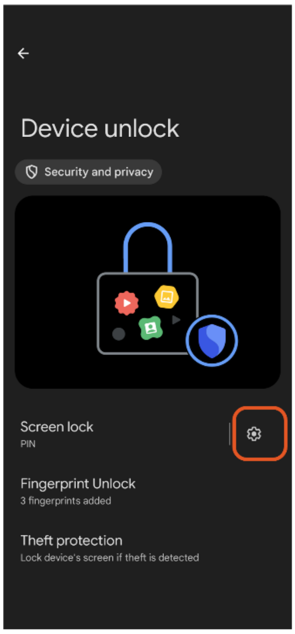
Device unlock
Screen lock, Fingerprint Unlock, Theft protection

Account security
Google Account is protected

Device finders
Find My Device

System and updates
Updates

4.



Device unlock

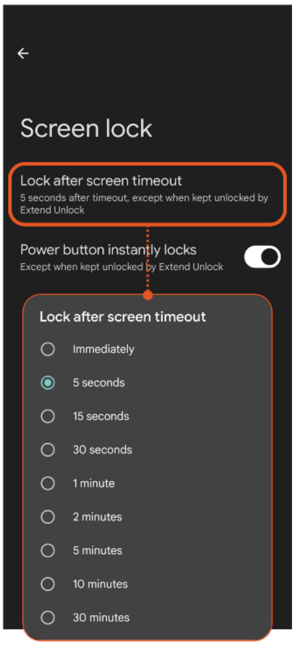
Security and privacy

Screen lock
PIN

Fingerprint Unlock
3 fingerprints added

Theft protection
Lock device's screen if theft is detected

5.



Screen lock

Lock after screen timeout
5 seconds after timeout, except when kept unlocked by Extend Unlock

Power button instantly locks
Except when kept unlocked by Extend Unlock

Lock after screen timeout

○ Immediately
● 5 seconds
○ 15 seconds
○ 30 seconds
○ 1 minute
○ 2 minutes
○ 5 minutes
○ 10 minutes
○ 30 minutes

5. TURN OFF EXTEND UNLOCK [*Extend Unlock*]

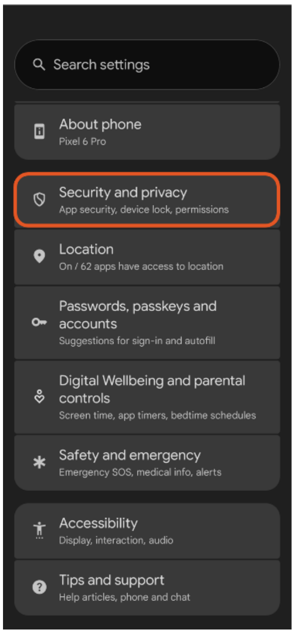
Extend unlock (formerly Smart Lock) is a quality of life feature of Android, which keeps your phone in an unlocked state when it detects that it is either in your pocket, connected to a trusted device or in a trusted location, such as your home. This can pose a significant security issue if your phone stays unlocked at the wrong time, or remains unlocked due to a connected device, such as Bluetooth headphones.

It is recommended that you disable this feature as the detection of 'your pocket' is triggered whenever you are moving in any way! Furthermore some Bluetooth devices stay connected to your phone all day (smartwatches) and so would keep your device unlocked all day if set as a trusted device.

To enable Advanced Protection:

- Step 1: Open 'Settings' (cog icon)
- Step 2: Select 'Security and Privacy'
- Step 3: Scroll down and select 'More security and privacy'
- Step 4: Scroll down and select 'Extend Unlock', you will be prompted to enter your passphrase.
- A brief notice may show telling you about what 'Extend Unlock' is.
- Step 5: Select and set the three options in turn as below:
  - 'On-body detection' left to off
  - 'Trusted Places' left to off
  - Remove any entries under 'Trusted devices'.

2.



Search settings

About phone
Pixel 6 Pro

Security and privacy
App security, device lock, permissions

Location
On / 62 apps have access to location

Passwords, passkeys and accounts
Suggestions for sign-in and autofill

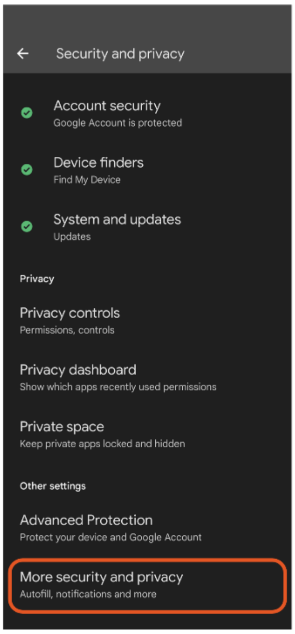
Digital Wellbeing and parental controls
Screen time, app timers, bedtime schedules

Safety and emergency
Emergency SOS, medical info, alerts

Accessibility
Display, interaction, audio

Tips and support
Help articles, phone and chat

3.



Security and privacy

Account security
Google Account is protected

Device finders
Find My Device

System and updates
Updates

Privacy

Privacy controls
Permissions, controls

Privacy dashboard
Show which apps recently used permissions

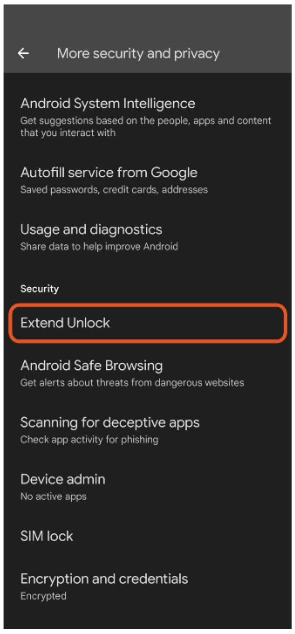
Private space
Keep private apps locked and hidden

Other settings

Advanced Protection
Protect your device and Google Account

More security and privacy
Autofill, notifications and more

4.



More security and privacy

Android System Intelligence
Get suggestions based on the people, apps and content that you interact with

Autofill service from Google
Saved passwords, credit cards, addresses

Usage and diagnostics
Share data to help improve Android

Security

Extend Unlock

Android Safe Browsing
Get alerts about threats from dangerous websites

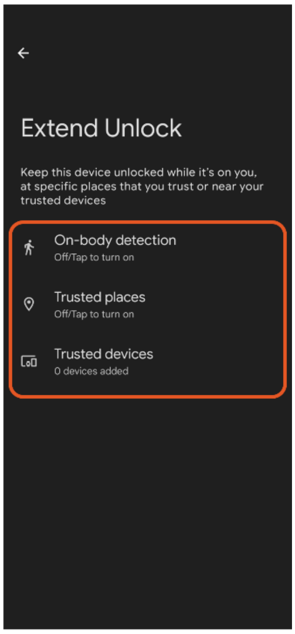
Scanning for deceptive apps
Check app activity for phishing

Device admin
No active apps

SIM lock

Encryption and credentials
Encrypted

5.



Extend Unlock

Keep this device unlocked while it's on you, at specific places that you trust or near your trusted devices

On-body detection
Off/Tap to turn on

Trusted places
Off/Tap to turn on

Trusted devices
0 devices added

6. DISABLE SHOW PASSWORDS [*Show passwords*]

With ‘Show passwords’ enabled password characters are shown briefly when you type, before changing to a dot (●), although this maybe helpful when entering a password, this can help anyone watching you type your password over your shoulder to learn it by character, rather than remembering just the keys you hit.

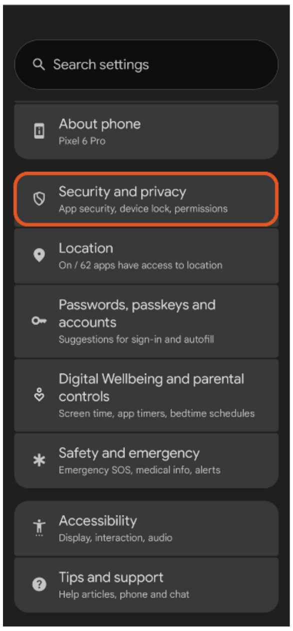
It is best to keep your passwords always hidden and only use the show password button for a few seconds to check a password is correct when necessary!

# Side Note: If you use a password manager, ensure that your password fields are set to hide the password, as they can still be compromised from viewing them in browser extensions/apps when auto filling.

To enable Advanced Protection:

- Step 1: Open ‘Settings’ ⚙ (cog icon)
- Step 2: Select ‘Security and Privacy’
- Step 3: Select ‘Privacy controls’
- Step 4: Scroll down to Controls and slide ‘Show passwords’ left to off.

2.



Search settings

About phone
Pixel 6 Pro

Security and privacy
App security, device lock, permissions

Location
On / 62 apps have access to location

Passwords, passkeys and accounts
Suggestions for sign-in and autofill

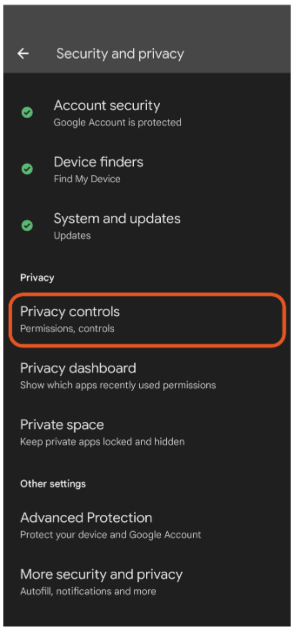
Digital Wellbeing and parental controls
Screen time, app timers, bedtime schedules

Safety and emergency
Emergency SOS, medical info, alerts

Accessibility
Display, interaction, audio

Tips and support
Help articles, phone and chat

3.



Security and privacy

Account security
Google Account is protected

Device finders
Find My Device

System and updates
Updates

Privacy

Privacy controls
Permissions, controls

Privacy dashboard
Show which apps recently used permissions

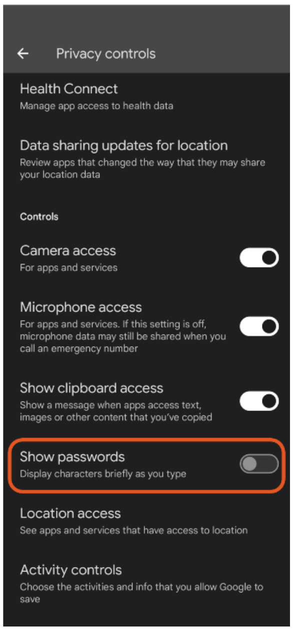
Private space
Keep private apps locked and hidden

Other settings

Advanced Protection
Protect your device and Google Account

More security and privacy
Autofill, notifications and more

4.



Privacy controls

Health Connect
Manage app access to health data

Data sharing updates for location
Review apps that changed the way that they may share your location data

Controls

Camera access
For apps and services

Microphone access
For apps and services. If this setting is off, microphone data may still be shared when you call an emergency number

Show clipboard access
Show a message when apps access text, images or other content that you've copied

Show passwords
Display characters briefly as you type

Location access
See apps and services that have access to location

Activity controls
Choose the activities and info that you allow Google to save

7. LOCK SCREEN INFORMATION & SECURITY [*Lock screen*]

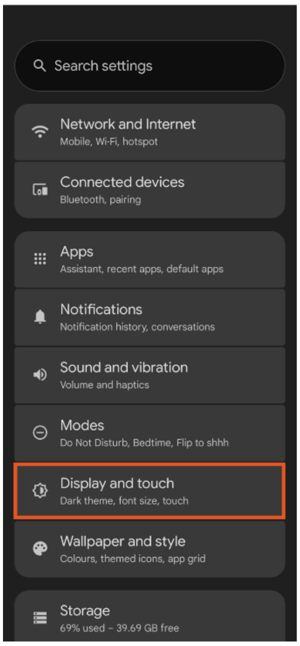
Your lock screen has many features of convenience, however these can make it easy to allow unauthorised access to your data, including messages, email and notifications, alongside banking information from Google Wallet (Google Pay).

The good news is you have a number of customisable options that allow you to still have some convenience without compromising the security of your data.

To configure what shows on the lock screen:

- Step 1: Open 'Settings' ⚙ (cog icon)
- Step 2: Select 'Display and touch
- Step 3: Next select 'Lock screen'
- Step 4: Select 'Privacy', an options menu will popup, select 'Show sensitive content only when unlocked', this will still give you notifications but with the content hidden.
  - Back on the lock screen page slide options below privacy left to off
  - Under shortcuts, only enable wallet if you have payment authentication on.
- Step 5: Back on the 'Display and touch' page select 'Screen timeout'
- Step 6: Select '15 seconds' and enable 'Screen attention' so that you screen lock 15 seconds after you look or move away form it.

2.



Search settings

Network and Internet
Mobile, Wi-Fi, hotspot

Connected devices
Bluetooth, pairing

Apps
Assistant, recent apps, default apps

Notifications
Notification history, conversations

Sound and vibration
Volume and haptics

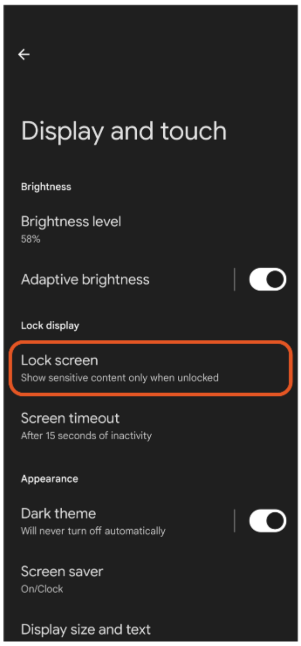
Modes
Do Not Disturb, Bedtime, Flip to shhh

Display and touch
Dark theme, font size, touch

Wallpaper and style
Colours, themed icons, app grid

Storage
69% used – 39.69 GB free

3.



Display and touch

Brightness

Brightness level
58%

Adaptive brightness — On

Lock display

Lock screen
Show sensitive content only when unlocked

Screen timeout
After 15 seconds of inactivity

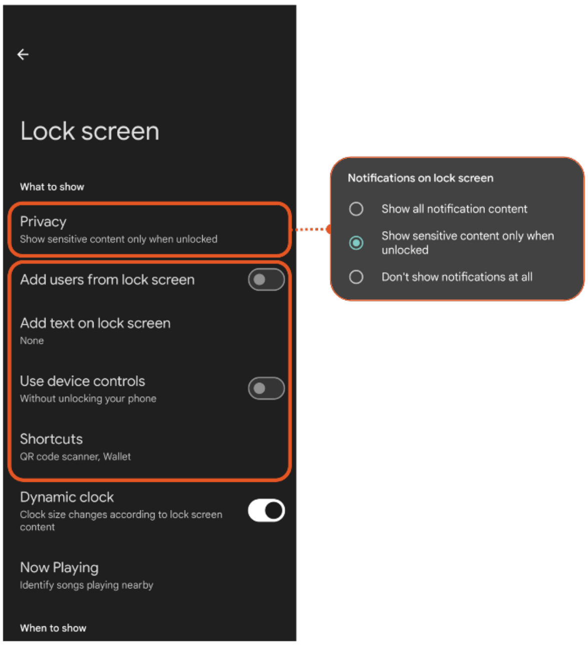
Appearance

Dark theme — On
Will never turn off automatically

Screen saver
On/Clock

Display size and text

4.



Lock screen

What to show

Privacy
Show sensitive content only when unlocked

Add users from lock screen — Off

Add text on lock screen
None

Use device controls — Off
Without unlocking your phone

Shortcuts
QR code scanner, Wallet

Dynamic clock — On
Clock size changes according to lock screen content

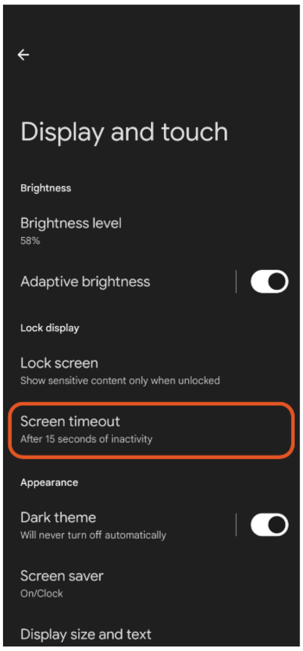
Now Playing
Identify songs playing nearby

When to show

Notifications on lock screen

○ Show all notification content
● Show sensitive content only when unlocked
○ Don't show notifications at all

5.



←

Display and touch

Brightness

Brightness level
58%

Adaptive brightness ☑

Lock display

Lock screen
Show sensitive content only when unlocked

Screen timeout
After 15 seconds of inactivity

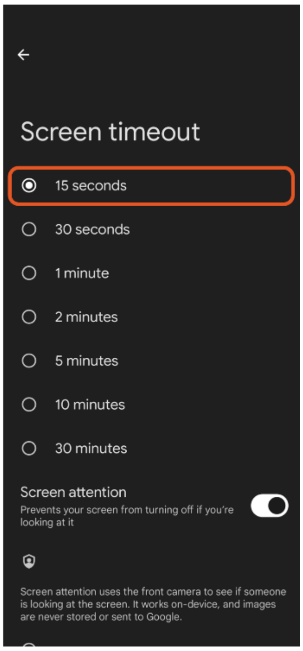
Appearance

Dark theme ☑
Will never turn off automatically

Screen saver
On/Clock

Display size and text

6.



←

Screen timeout

● 15 seconds

○ 30 seconds

○ 1 minute

○ 2 minutes

○ 5 minutes

○ 10 minutes

○ 30 minutes

Screen attention ☑
Prevents your screen from turning off if you're looking at it

Screen attention uses the front camera to see if someone is looking at the screen. It works on-device, and images are never stored or sent to Google.

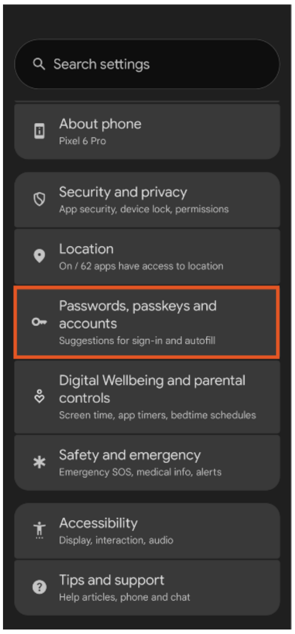
8. PREVENT STORING PASSWORDS, PASSKEYS & BANKING DETAILS [*Password Manager*]

You should only be storing any passwords, Banking information and any other personal information in a password manager and not in your Google account, any autofill functionality or a browser. An exception to this is Google Wallet which possesses better security and authentication.

To disable your phone asking to remember everything:

- Step 1: Open 'Settings' ⚙ (cog icon)
- Step 2: Select 'Passwords, passkeys and accounts'
  - In this section you can see all your accounts and set your preferred password manager, using the 'change' button. (Don't use Google)
- Step 3: Slide the toggle left to off, this disables the prompts to remember info.
  - Then select 'Google' under additional services
- Step 4: Now select 'Google Password Manager' and select 'Settings' on the screen that appears.
  - The 'Google Pay' option on this screen will allow you to remove stored banking cards from Google Wallet/Pay.
- Step 5: Slide the top four toggles 'left' to off, to prevent storing of passwords and automatic logging in of accounts.
  - If you think you have any data stored in Google you can use the 'Export' function to retrieve them and then you should select the 'Delete all data'.

2.



Search settings

About phone
Pixel 6 Pro

Security and privacy
App security, device lock, permissions

Location
On / 62 apps have access to location

Passwords, passkeys and accounts
Suggestions for sign-in and autofill

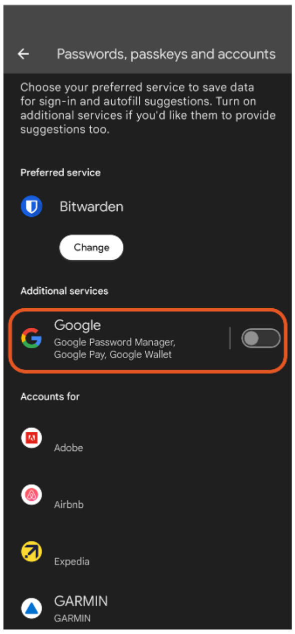
Digital Wellbeing and parental controls
Screen time, app timers, bedtime schedules

Safety and emergency
Emergency SOS, medical info, alerts

Accessibility
Display, interaction, audio

Tips and support
Help articles, phone and chat

3.



Passwords, passkeys and accounts

Choose your preferred service to save data for sign-in and autofill suggestions. Turn on additional services if you'd like them to provide suggestions too.

Preferred service

Bitwarden

Change

Additional services

Google
Google Password Manager, Google Pay, Google Wallet

Accounts for

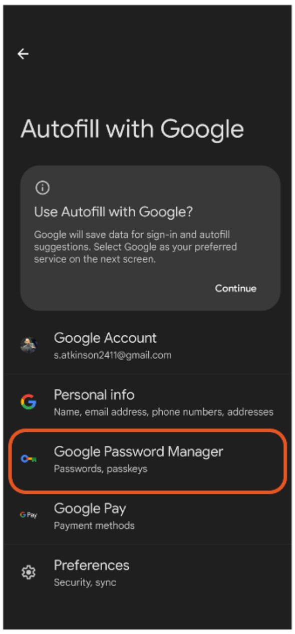
Adobe

Airbnb

Expedia

GARMIN
GARMIN

4.



Autofill with Google

Use Autofill with Google?
Google will save data for sign-in and autofill suggestions. Select Google as your preferred service on the next screen.
Continue

Google Account
s.atkinson2411@gmail.com

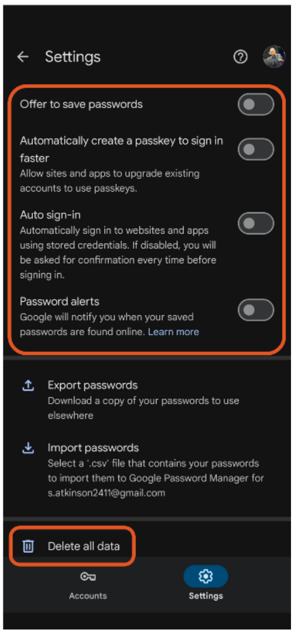
Personal info
Name, email address, phone numbers, addresses

Google Password Manager
Passwords, passkeys

Google Pay
Payment methods

Preferences
Security, sync

5.



Settings

Offer to save passwords

Automatically create a passkey to sign in faster
Allow sites and apps to upgrade existing accounts to use passkeys.

Auto sign-in
Automatically sign in to websites and apps using stored credentials. If disabled, you will be asked for confirmation every time before signing in.

Password alerts
Google will notify you when your saved passwords are found online. Learn more

Export passwords
Download a copy of your passwords to use elsewhere

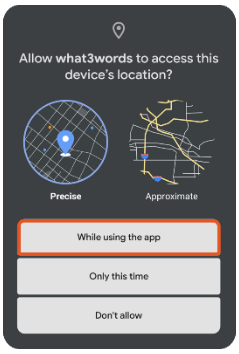
Import passwords
Select a '.csv' file that contains your passwords to import them to Google Password Manager for s.atkinson2411@gmail.com

Delete all data

Accounts
Settings

9. APP PERMISSIONS [*Search*]

Android offers the ability to control, Location, Camera, Contact and many more permissions for apps individually. By default it is best practice to only allow a permission while you are using an app, unless the app is something that runs all the time in the background such as a password manager or weather app. Luckily android makes this easy, as when you install an app and run it for the first time, it will ask for the permissions it needs to run, not all options will specify a 'While using the app' option, such as access to contacts or files, however active services such as location do:



Allow **what3words** to access this device's location?

Precise

Approximate

While using the app

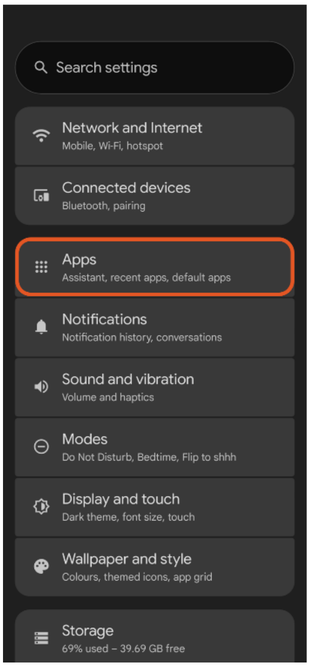
Only this time

Don't allow

To review the permission of an App:

- Step 1: Open 'Settings' (cog icon)
- Step 2: Select 'Apps'
- Step 3: Select the app you want to check, select 'See all ### apps' if your app isn't listed in the recently opened list
- Step 4: Now select 'Permissions' where you will see all the permissions and their settings for that specific App.

2.



Search settings

Network and Internet
Mobile, Wi-Fi, hotspot

Connected devices
Bluetooth, pairing

Apps
Assistant, recent apps, default apps

Notifications
Notification history, conversations

Sound and vibration
Volume and haptics

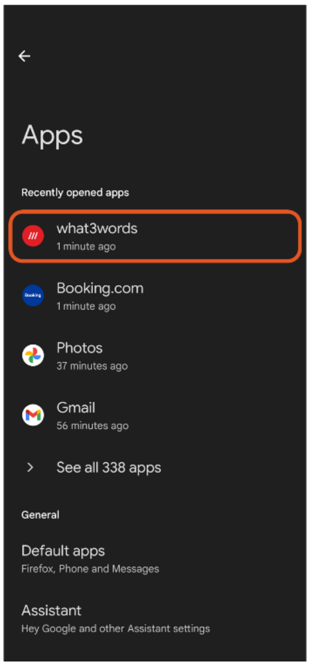
Modes
Do Not Disturb, Bedtime, Flip to shhh

Display and touch
Dark theme, font size, touch

Wallpaper and style
Colours, themed icons, app grid

Storage
69% used – 39.69 GB free

3.



Apps

Recently opened apps

what3words
1 minute ago

Booking.com
1 minute ago

Photos
37 minutes ago

Gmail
56 minutes ago

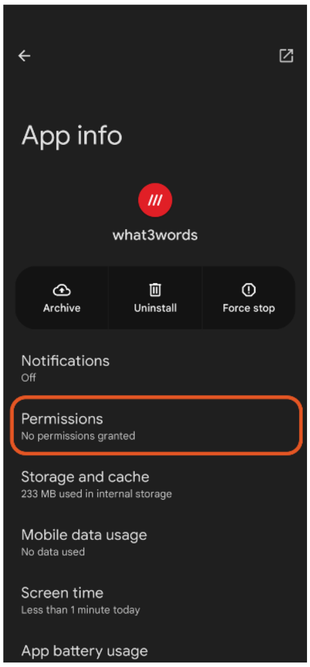
See all 338 apps

General

Default apps
Firefox, Phone and Messages

Assistant
Hey Google and other Assistant settings

4.



App info

what3words

Archive | Uninstall | Force stop

Notifications
Off

Permissions
No permissions granted

Storage and cache
233 MB used in internal storage

Mobile data usage
No data used

Screen time
Less than 1 minute today

App battery usage

10. DISSABLE WIFI SCANNING [*Wi-Fi scanning*]

Google provides WiFIManager feature to the location services and app developers, which continually scans for any of the known networks (any you have joined at least once) within the vicinity of the device, even if WiFi is turned off! It also uses known public networks to aid in location accuracy.

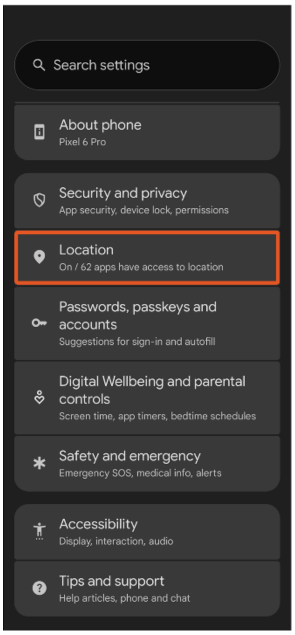
This is dangerous as your phone is essentially announcing openly every WiFi network it knows and can be used to make your phone think it's connecting to it's home network, and when used for location allows your location data to be utilised by data brokers.

Disabling the ability to scan in the background and when WiFi is off helps prevent this.

To disable WiFi Scanning:

- Step 1: Open 'Settings' ⚙ (cog icon)
- Step 2: Select 'Location'
- Step 3: Then Select 'Location Services'
- Step 4: Scroll down and select 'Wi-Fi scanning'
- Step 5: Slide the 'Wi-Fi Scanning' left to off.

2.



Search settings

About phone
Pixel 6 Pro

Security and privacy
App security, device lock, permissions

Location
On / 62 apps have access to location

Passwords, passkeys and accounts
Suggestions for sign-in and autofill

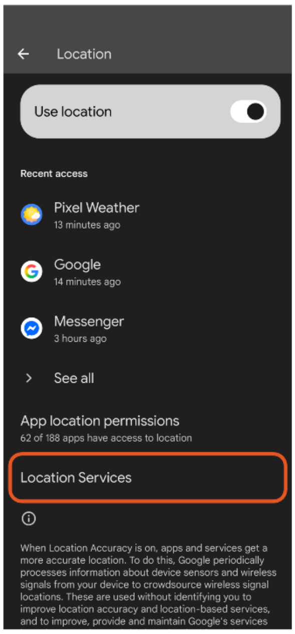
Digital Wellbeing and parental controls
Screen time, app timers, bedtime schedules

Safety and emergency
Emergency SOS, medical info, alerts

Accessibility
Display, interaction, audio

Tips and support
Help articles, phone and chat

3.



Location

Use location ●

Recent access

Pixel Weather
13 minutes ago

Google
14 minutes ago

Messenger
3 hours ago

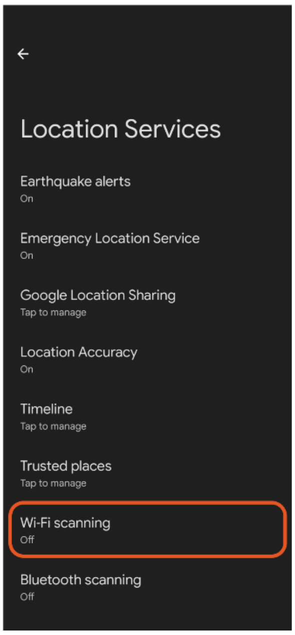
See all

App location permissions
62 of 188 apps have access to location

Location Services

When Location Accuracy is on, apps and services get a more accurate location. To do this, Google periodically processes information about device sensors and wireless signals from your device to crowdsource wireless signal locations. These are used without identifying you to improve location accuracy and location-based services, and to improve, provide and maintain Google's services

4.



Location Services

Earthquake alerts
On

Emergency Location Service
On

Google Location Sharing
Tap to manage

Location Accuracy
On

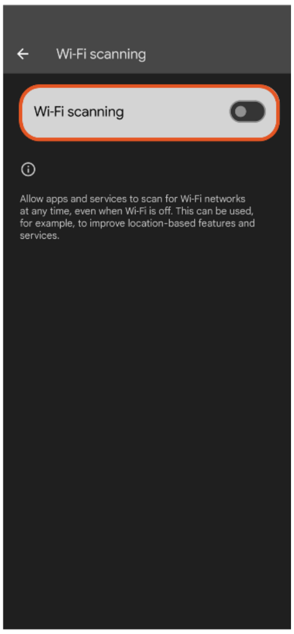
Timeline
Tap to manage

Trusted places
Tap to manage

Wi-Fi scanning
Off

Bluetooth scanning
Off

5.



Wi-Fi scanning

Wi-Fi scanning ○

Allow apps and services to scan for Wi-Fi networks at any time, even when Wi-Fi is off. This can be used, for example, to improve location-based features and services.