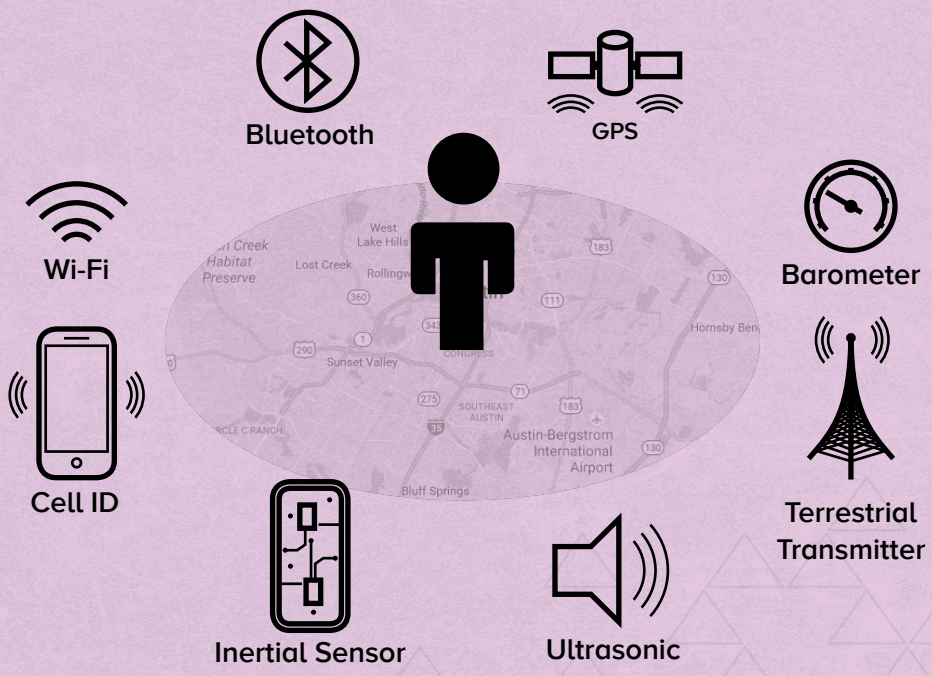
A SECURE PHONE IS ALWAYS THE FOUNDATION!

Your phone is one of the most critical components of your digital ecosystem. Phones are essential to communication, strategizing, and community organization. Most people communicate primarily through their mobile phone, followed by their computers and tablets. However, for these very reasons, governments and corporations throughout the world use data collected through our phones to perform extensive surveillance.

As useful as it is, your phone can present pathways to serious violations of your privacy and security. Below is a graphic that shares all the different ways it collects and shares your personal data with cell phone service providers and phone manufactures. This vulnerability may allow governments and hackers to access information about your physical location at any time, **even when it's turned off**.

WARNING: Governments or malicious actors can turn on your phone's microphone and camera to listen to you even when the device is turned off?



Today, law enforcement agencies use technology that provide police with data about the identity, activity, and location of any phone that connects to targeted cell phone towers over a set span of time. A typical broad data search covers multiple towers and wireless providers and can net information from thousands of phones—without need for warrants.[10]

Organizations such as the American Civil Liberties Union (ACLU) and Electronic Privacy Information Center (EPIC), say that the power of even small-town police departments to quickly obtain cell phone data results in the erosion of privacy and the violation of Fourth Amendment protections against unreasonable search and seizure. But thanks to a unanimous Supreme Court decision in Riley v. California, this practice is now officially legal.[11]

In extreme circumstances, **to prevent all tracking of your location from your phone, shut it down completely and remove the battery. This is the easiest way to ensure that you can't be tracked**, But it comes at the price of not being able to use your phone at all. If you need access to any data on your phone, back it up to a computer before you power down your device.

If your phone's battery cannot be removed, place it in a **faraday bag,** which blocks transmission with its internal lining.[12] Not all faraday bags are created equal, so make sure you try it out before you put it into use in everyday life. You want to confirm that, at a minimum, cell and GPS services are blocked.

In addition to these scenarios, we face threats of information leaks during the everyday use of our phones. There are several simple safe practices that can be adopted to keep ourselves and our information safe. In the following section, we will explore a few of them.

NOTE: The "Secure Your Phone" section is broken up to address actions for Androids and iPhones separately. Please find the section that works for your device and begin.

[6] http://www.usatoday.com/story/news/nation/2013/12/08/cellphone-data-spying-nsa-police/3902809/

[7] https://www.eff.org/deeplinks/2014/08/cell-phone-guide-protesters-updated-2014-edition

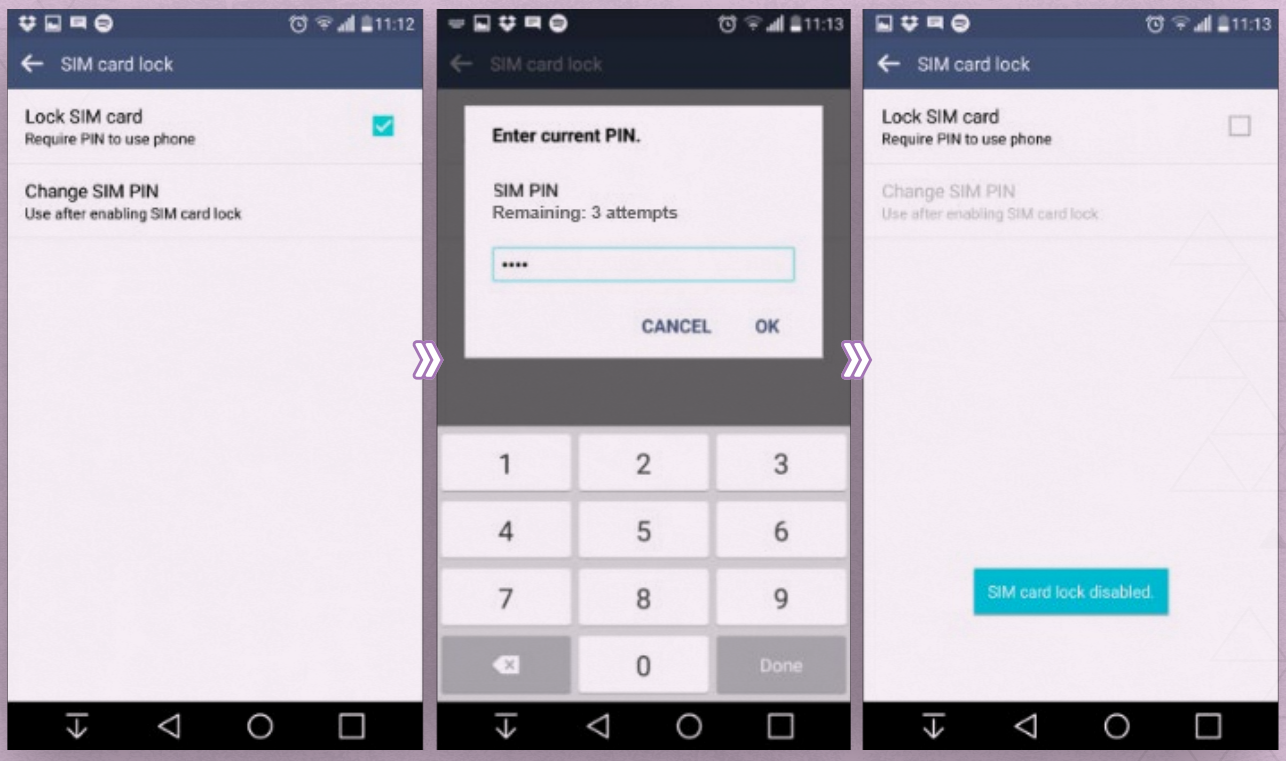
[8] https://www.amazon.com/Black-Hole-Faraday-Bag-Anti-tracking/dp/B0091WILY0

SECURE YOUR ANDROID

1. LOCK YOUR SIM

If your phone uses a SIM card, you can set a lock on the card so it cannot be used by anyone who does not know the code. If your SIM is stolen, this measure can protect your identity.

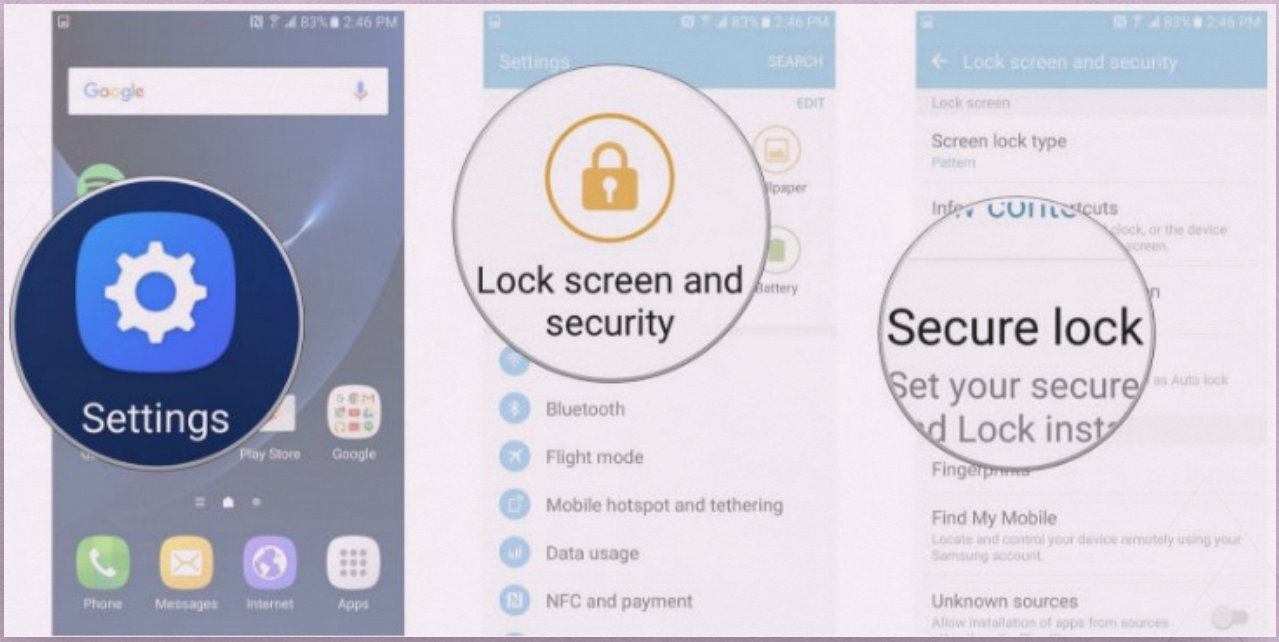
- ☑ Enable Lock SIM card by going to **Settings → Personal → Security → Set up SIM card lock**. Now, each time your phone is turned on it will require a PIN in order to unlock your SIM card. No one will be able to make calls using your device without the PIN.



2. SET UP YOUR PIN AND ACTIVATE A SCREENLOCK

- Set up a screen lock by accessing **Settings → Personal → Security → Screen Lock**, to ensure that lists, pictures, and a code, pattern, or password need to be entered in order to unlock the screen.

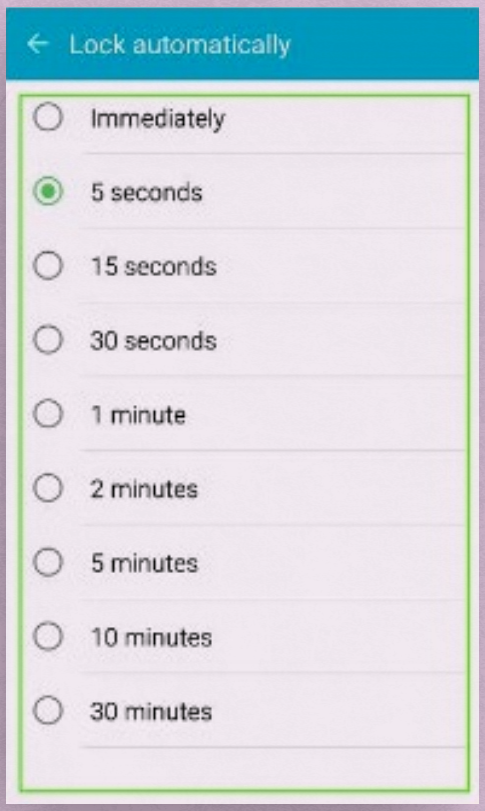
We recommended using the PIN or password option, as these are more obstructive to law enforcement or adversaries than a fingerprint ID. This measure is particularly important in the event that you are faced with a casual search by police or other authorities.



NOTE: We highly recommend that people **DO NOT** use the fingerprint login, as you could be forced or manipulated into putting your finger on your screen. There are also more legal protections for the PIN versus the fingerprint login or even swipe access to one's phone. Finally it is never a good idea to give your biometric data like a fingerprint to a corporation if you can avoid it. So when in doubt use a PIN!

3. ACTIVATE A SECURITY LOCK TIMER

- Set the security lock timer, which will automatically lock your phone after a certain amount of time.
- Go to **Settings → Display → Sleep.** Different versions of the firmware use different names for this menu so you will have to find the one that matches your phone.
- Now select a time period that is appropriate to your usage habits in the pop-up menu that appears. The change will take place immediately.



For maximum security, always choose the shortest possible timeframe that suits you without becoming too taxing. You can always adapt your times to your activities as well. So if you use your phone for recipies keep security lock timer off, but then turn it back on when you resume regular activity. Use your risk assessment to figure out what makes the most sense for you.

4. ANDROID ENCRYPTION

With Androids, encrypting your phone is one of the best ways to protect your data if the device is ever stolen, seized, or confiscated. The purpose of encryption is to ensure that only someone who is authorized to access your phone's data will be able to read it using the decryption key.

When your phone is encrypted, its data is stored in an unreadable, seemingly scrambled form. If your phone is stolen, confiscated, or lost, this feature can protect data like your home address, email, bank accounts, communications, etc.

When you enter your PIN or your pattern on the lock screen, your phone decrypts the data, making it understandable and accessible to you. Without the encryption PIN or password, a malicious actor can't access your data. This is why Encryption is one of key building blocks of securing your phone.

NOTE: Before starting the encryption process, ensure your phone is backed up, fully charged, and plugged into a power source. This ensures that the encrypting process is not interrupted. If it is interrupted, and your data is lost or damaged, you will have a backup of all of your data.

- To begin encryption find out whether or not your Android has Encryption enabled. Some versions of Android come with Encryption already set up while others need to set it up manually. To discover where your phone is at please first visit **Settings → Personal → Security → Encryption**.

- If Encryption is enabled it will say it here clearly. If not then your next step will require you to set a screen lock password (described above).

- Once your PIN is selected make sure you phone is fully charged and backed up as you will not want to disturb the Encryption process. A back up also ensures that if anything goes wrong during encryption that your data is protected and your phone can be restored.

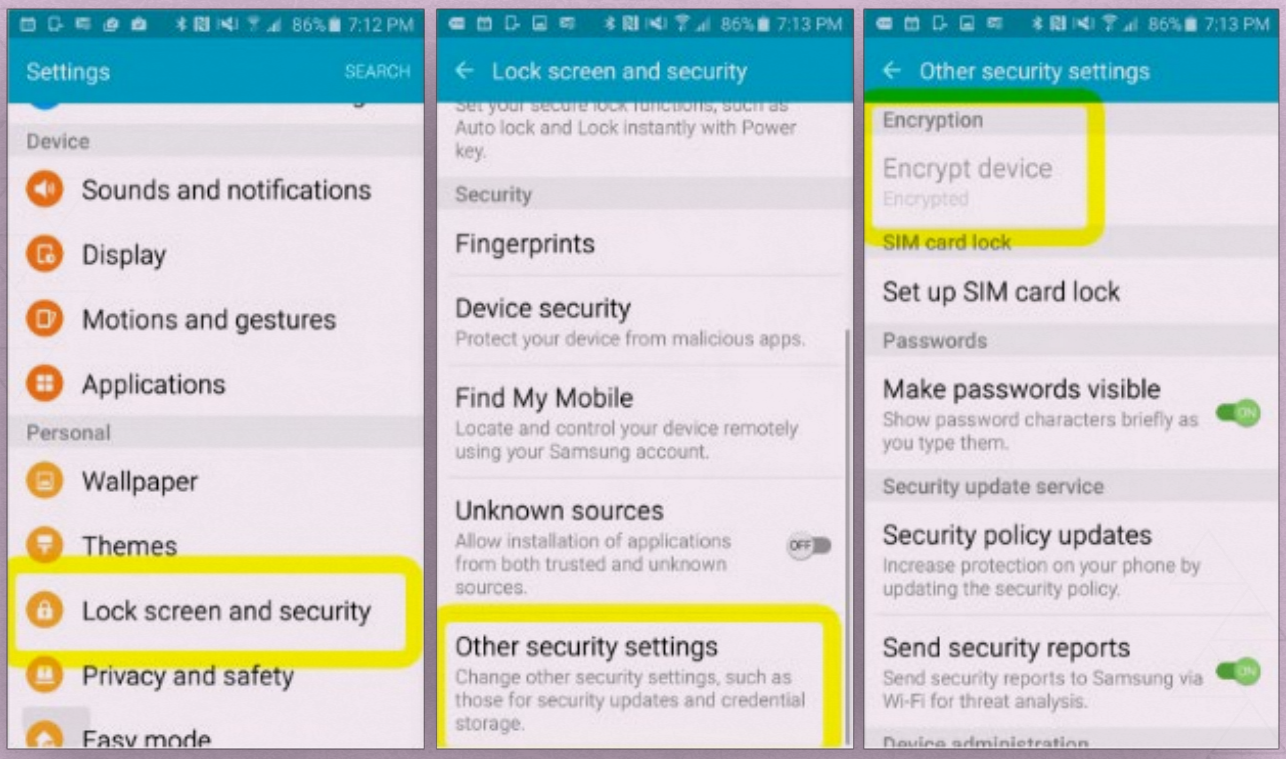
- Once the phone is ready and plugged in, please begin Encrypting by hitting Encrypt. The process should last anywhere from 30min to a couple of hours.

5. ADJUST YOUR NETWORK SETTINGS

We recommend keeping most networks turned off and only manually enabling them when necessary. One example is Bluetooth. Also, ensure that tethering and portable hotspots are switched off when not in use.

- Do so by accessing **Settings → Wireless & Networks → More → Tethering & Mobile Hotspot**.

If your device supports Near Field Communication (NFC), it will be switched on by default and must be disabled manually.



6. YOUR LOCATION SETTINGS

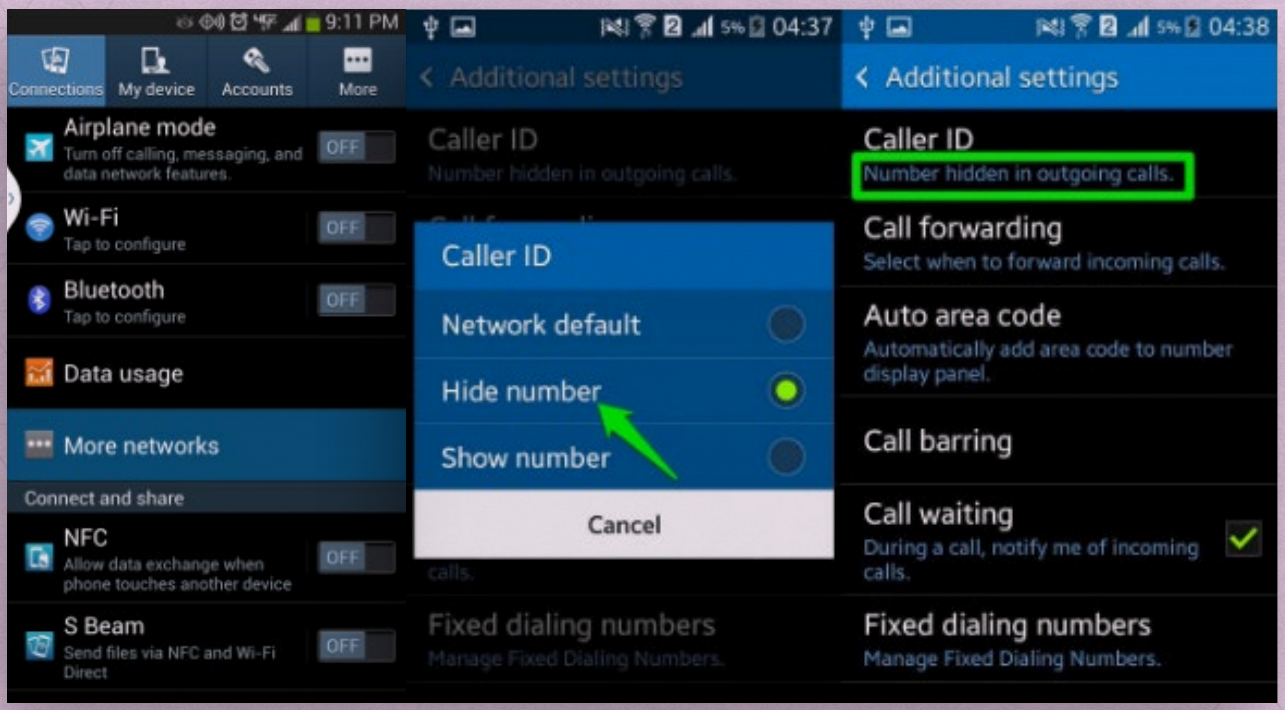
- Switch off wireless and GPS location (under Location Services) and mobile data (under **Settings → Personal → Location**)

NOTE: Only turn on location settings if necessary. When these services aren't running by default in the background, it reduces the risk of location tracking, saves battery power, and prevents unwanted data streams initiated by applications or your mobile carrier.

HIDING CALLER ID

You can hide your phone number from showing up to the person you are calling. However, you should note that your phone carrier and legal authorities will still have full access to logs showing who you called and when.

- Go to Settings and then tap on **Call → Additional Settings → Caller ID → Hide Number and it will be blocked**.



7. UPDATE YOUR ANDROID

To ensure that your phone remains secure, we strongly recommend you keep your software updated. There are two types of updates to check for:

- The phone's operating system: Go to **Settings → About phone → Updates → Check for Updates**[13]
- Individual apps you have installed: Open the **Google Play Store app**, and select My Apps from the side menu.

NOTE: It is important to always update your phone's software from a trusted location—such as your internet connection at home—somewhere like an internet cafe or coffee shop.

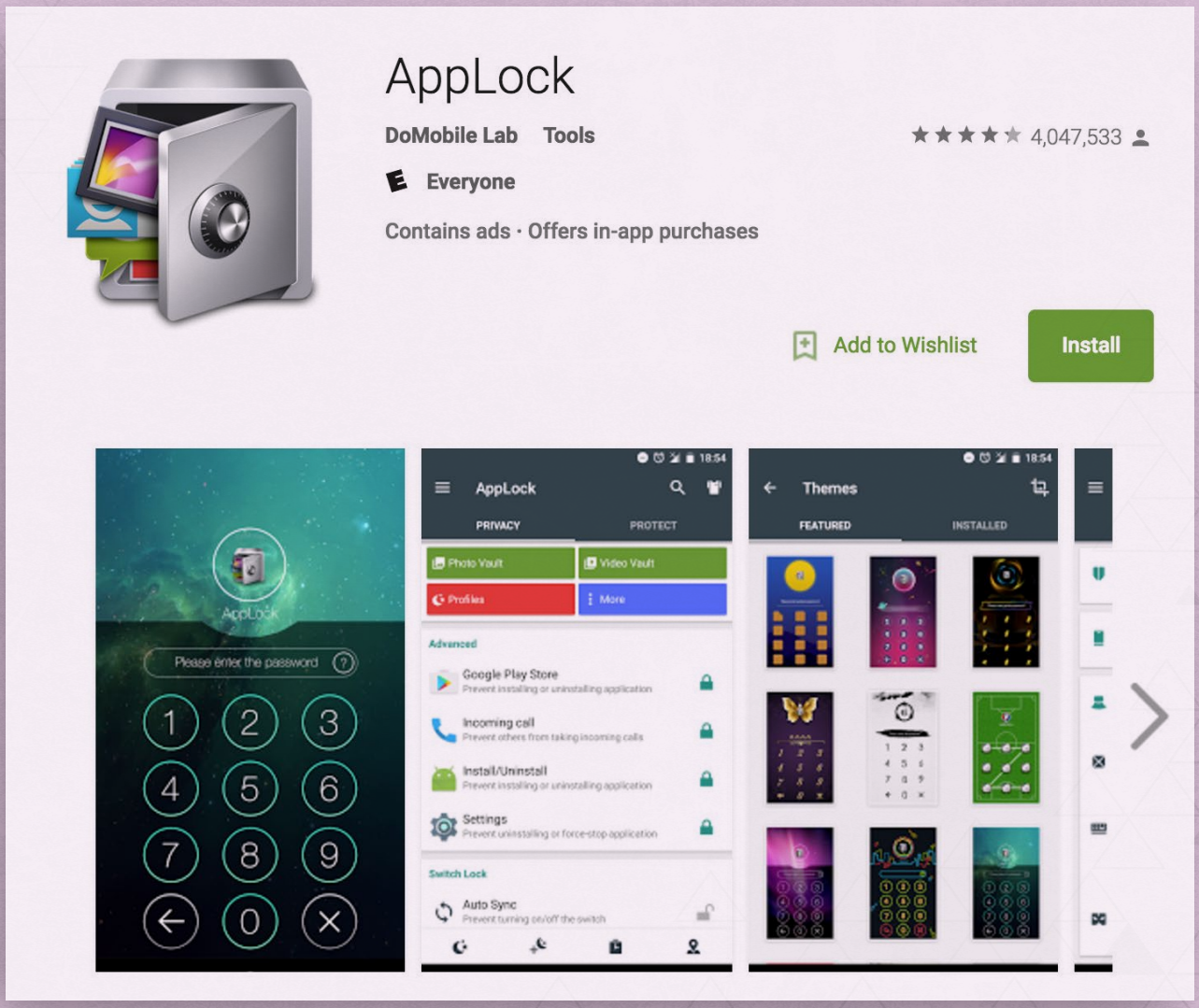
[9] https://videotron.tmtx.ca/en/topic/google_nexus6p/hiding_your_phone_number.html

1. APPLOCK FOR ANDROIDS

Security needs can arise in simple scenarios, such as keeping prying eyes out of certain apps. You might hand your phone to someone so they can make a call or look at a picture. You might be stopped by the police or have your phone confiscated. Once you turn your back, it's easy for that user to dig into your data.

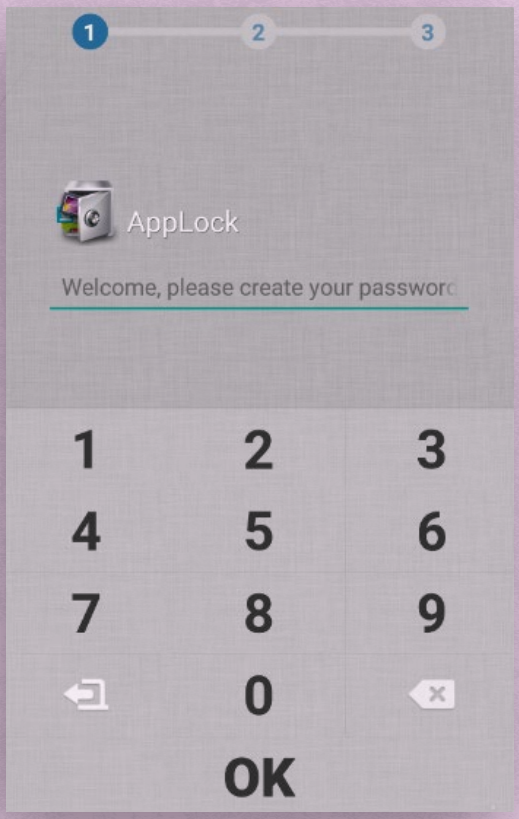
Fortunately, there are ways to keep certain applications readily available while others are locked down. Keeping a password lock on your phone prevents casual snooping through your contact numbers, texts, and data. In addition to requiring a passcode to unlock your phone, you can also download software that allows you to set a code for individual apps.

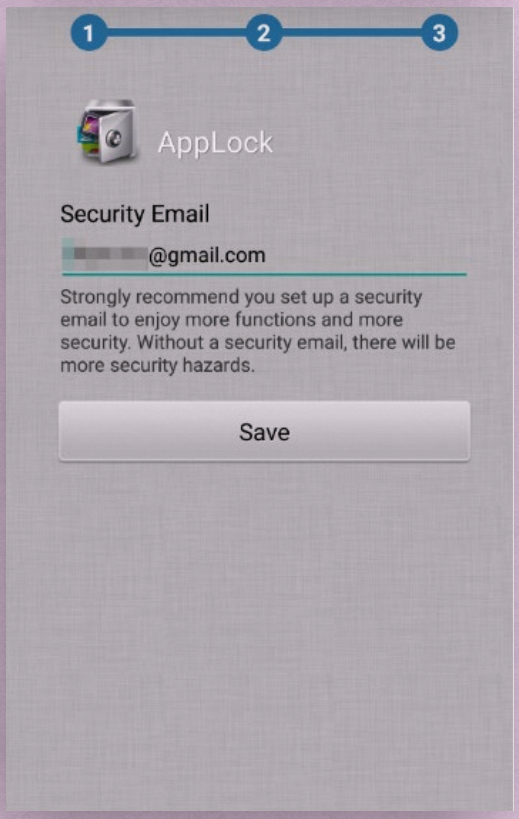
We recommend using **AppLock**[10] on Androids. AppLock is a free app that extends your phone's access controls to specific applications.



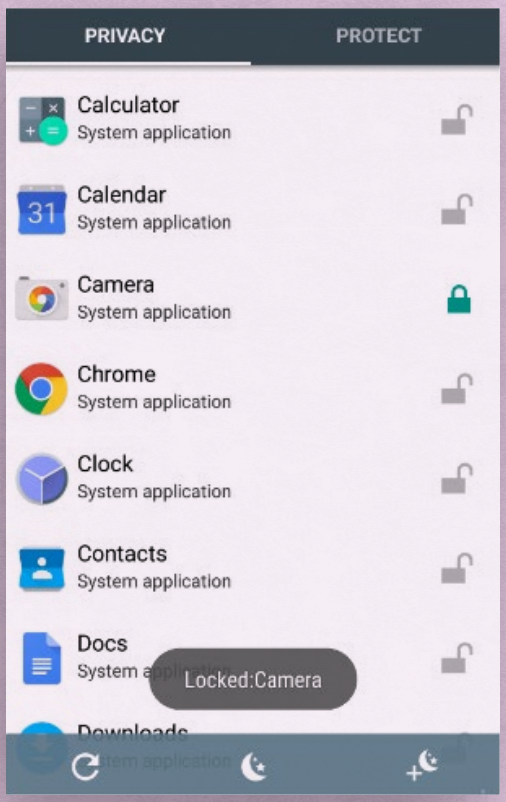
[10] https://play.google.com/store/apps/details?id=com.domobile.applock&hl=en

- Once you download, install, and open AppLock, you will be prompted to create a password. This is used whenever you re-open AppLock, as well as when you want to access any of the apps you will be protecting, so make sure it's a password you can easily remember. You'll also need to provide a security e-mail address.

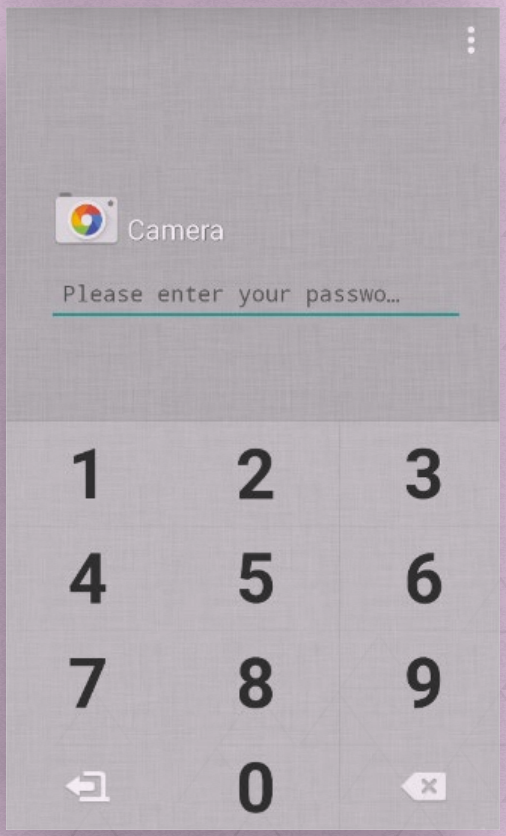




- After that, you are all set to start locking individual apps, such as Phone, Messenger, Facebook, and so on. If you want to lock the Camera app, for example, you'll simply tap the lock icon.



- Now it is locked, and if you want to access your phone's camera, you will be prompted to enter your passcode.



2. DEALING WITH METADATA ON PHOTOS

Photos we take on all electronic devices can often carry data that can be used to pinpoint our location and gather other information about us.

This information can be intercepted and gathered as part of the surveillance of our movements and habits. These details are often shared through something called **metadata** which is the additional details useful to categorizing, locating, or describing a file. Put simply, metadata refers to data about data.

Many of the files we use and create on our phones have metadata, including emails, text messages, and photos. So one of the ways we can secure our phones is by minimizing the metadata our phones share while we communicate.

The metadata in photographs are known as the **Exchangeable Image File Format,** or **EXIF.** This can reveal much about you, your subject, and where a photo was taken. Metadata embedded in a photo includes the following:

- Key identifying information, such as camera or cell phone user, GPS coordinates, and the time and date the photo was taken.
- Camera settings, including static information such as the camera model and make, and information that varies with each image such as orientation (rotation), aperture, shutter speed, focal length, metering mode, and ISO speed information.
- A thumbnail preview of the picture on the camera's LCD screen, in file managers, or in photo manipulation software.
- Descriptions of a photograph's content.
- Copyright information.

NOTE: Different versions of Android may have different ways to get to the settings described in this section. We describe the general method but do a little searching around the settings areas of your particular version of phone to make sure you achieve the same.

SWITCH OFF LOCATION TAGGING FOR YOUR CAMERA

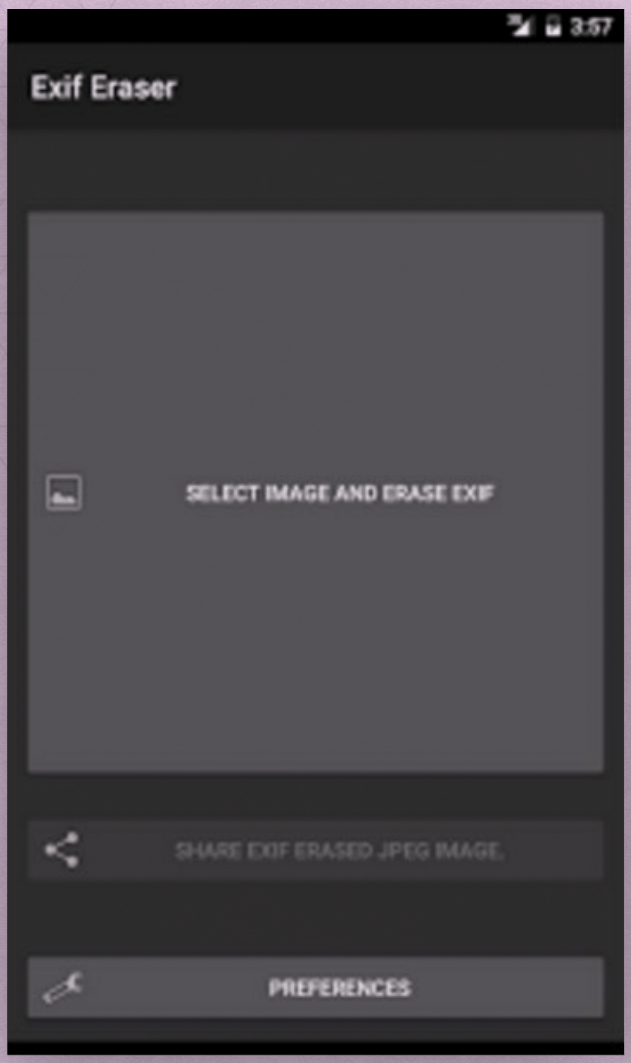
Android: Open the **Camera** app and tap the circle to the right of the shutter button. From the resulting menu, tap the **Settings** icon. Now, in the settings menu, tap the “Location” button. You can tell that geolocation is now disabled because of the icon overlaid on the options button.

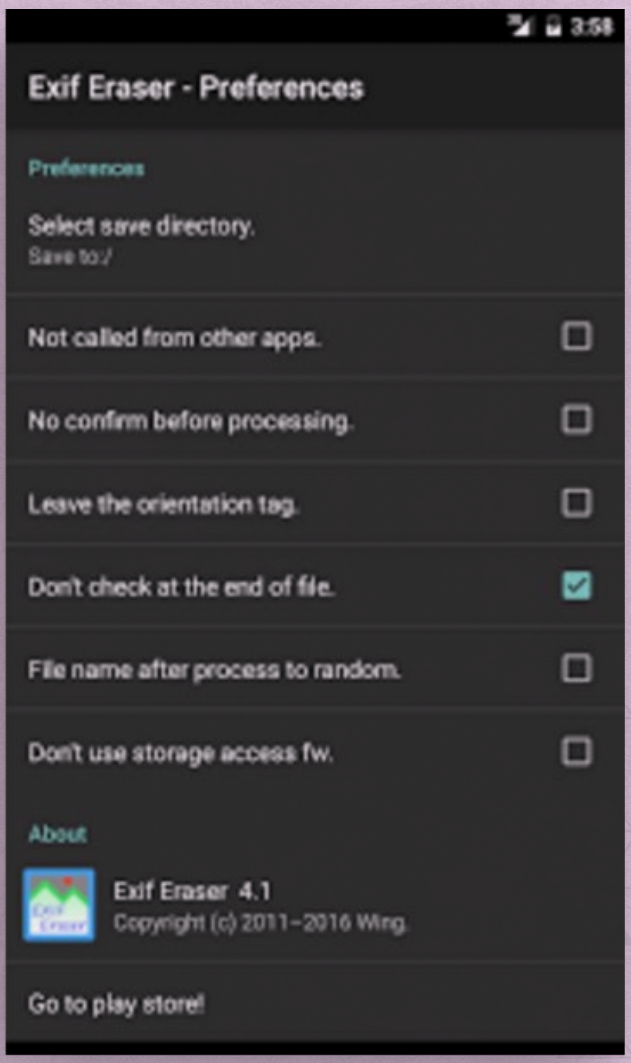
INSTALL A THIRD-PARTY APP FOR SCRUBBING METADATA FROM IMAGES

To remove (“scrub”) existing metadata from images we have taken on our Androids we can use third-party apps For Android we recommend installing and using **Exif Eraser**.

Exif Eraser for Android
After installing Simply pick one or more photos with EXIF information from Gallery or the app.

- Choose whether you want to replace the photo, create a new copy, or simply share the photo (e.g. to Facebook).
- Then, you are free to share your EXIF-free photos without compromising your privacy.



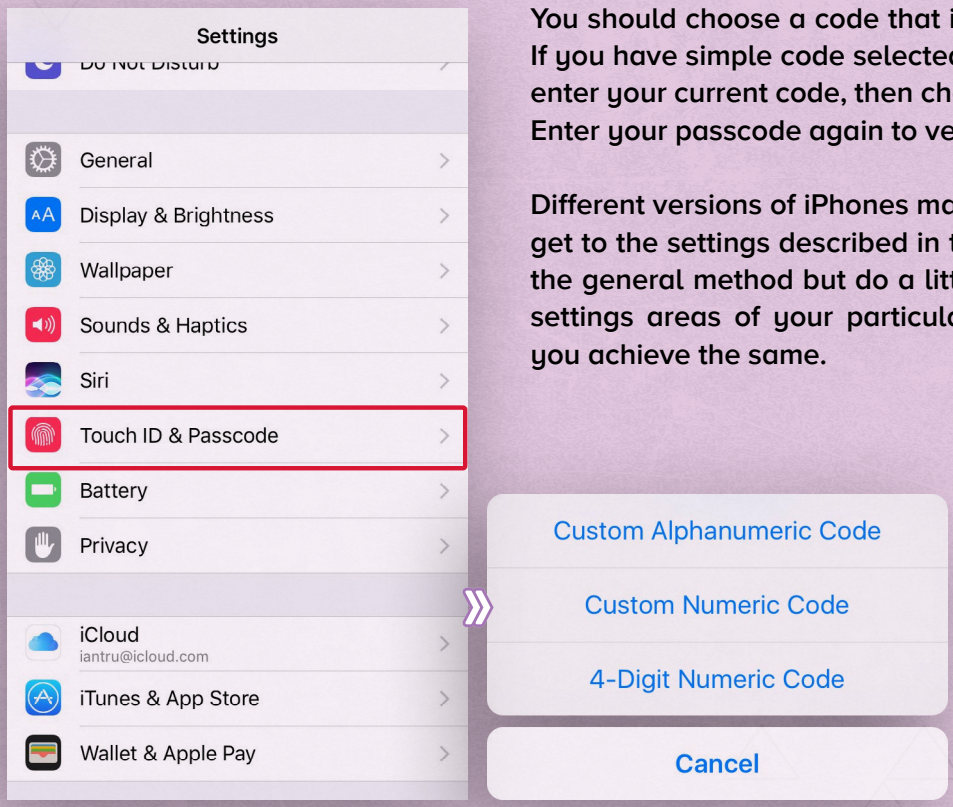


SECURE YOUR IPHONE

1. ACTIVATE YOUR SCREEN LOCK

First, set up a passcode. Some phones also allow you to set your fingerprint as your password through Touch ID.[11] We do not recommend setting up Touch ID, as you can be physically, unwillingly compelled to open your device. Instead, simply set a strong PIN.

- ✓ To set these up, go to **Settings → Touch ID & Passcode**. On devices without Touch ID, go to **Settings → Passcode**.
- ✓ Tap **Turn Passcode On**. Then, tap **Passcode Options** to switch to a four-digit numeric code, a custom numeric code, or a custom alphanumeric code.



You should choose a code that is at least six digits long. If you have simple code selected, tap Change Passcode, enter your current code, then choose a harder sequence. Enter your passcode again to verify and activate it.

Different versions of iPhones may have different ways to get to the settings described in this section. We describe the general method but do a little searching around the settings areas of your particular version to make sure you achieve the same.

[11] http://www.pcadvisor.co.uk/how-to/mobile-phone/how-to-set-up-a-sim-lock-on-an-apple-iphone-3304041/

WARNING: We highly recommend that you DO NOT use a fingerprint login, as you can be unwillingly compelled to place your finger on the home button.

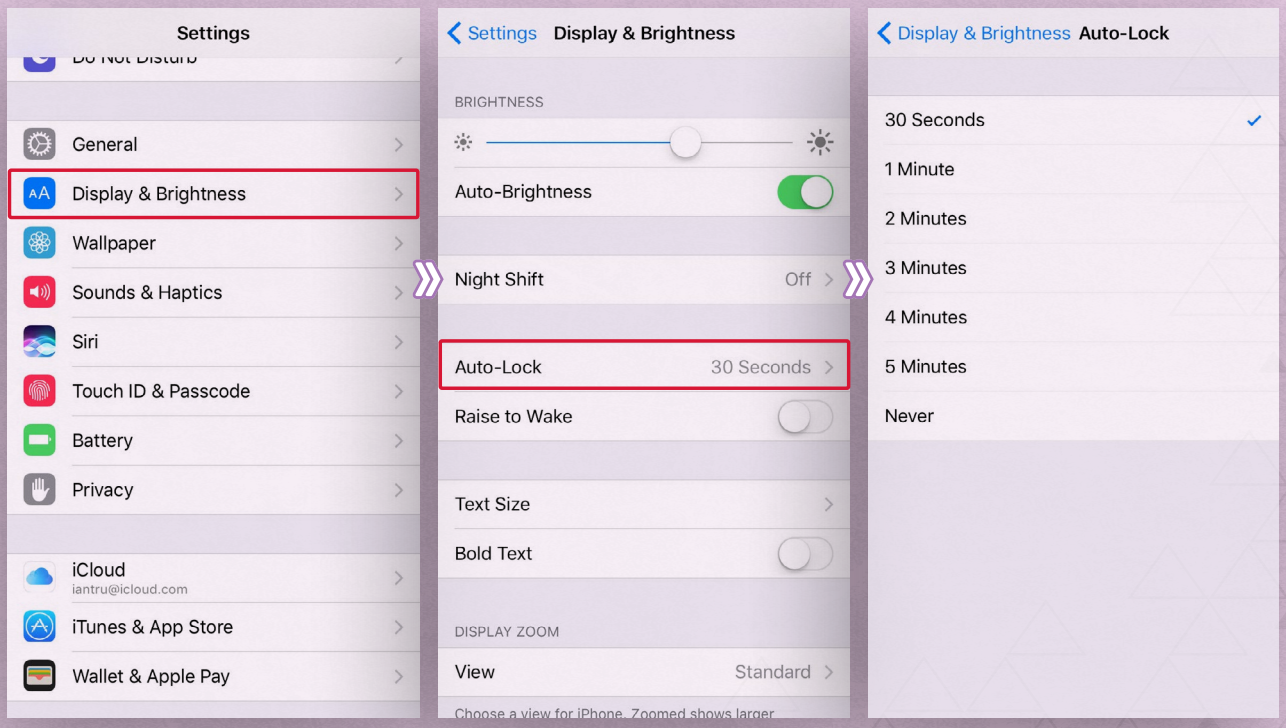
2. ACTIVATE YOUR SECURITY LOCK TIMER

- Go to the **Settings → Display & Brightness → Auto-Lock**.

- **Choose the time interval.** This means that, if you have not used your phone for the amount of time specified, it will automatically lock. Do not choose **"Never"**, as that will leave you vulnerable; instead, select an interval **between 30 seconds and one minute**.

  For maximum security, always choose the shortest possible timeframe that suits you without becoming too taxing. You can always adapt your times to your activities as well. So if you use your phone for recipies keep security lock timer off, but then turn it back on when you resume regular activity. Use your risk assessment to figure out what makes the most sense for you. If necessary, you can change it to a longer interval to complete a specific task, but make sure you change it back!

- If you are running iOS 9 or iOS 8, the lock screen option is available in **Settings → General → Auto-Lock → Time interval**.[12]



[12] http://www.howtoisolve.com/turn-on-off-change-auto-lock-screen-time-iphone/

3. IPHONE ENCRYPTION

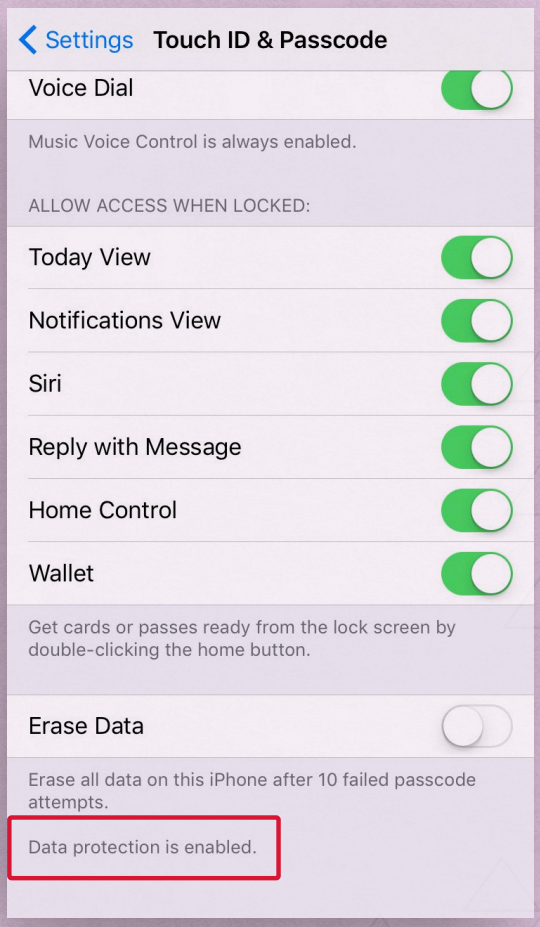
Encryption is essentially one of the best was to protect your phone's data if it is stolen, seized, or confiscated. The purpose of encryption is to ensure that only somebody who is authorized to access data will be able to read it, using the decryption key.[13]

With Androids, you must enable device encryption, but most modern Apple devices encrypt their contents by default, with varying levels of protection. However, to protect yourself from someone obtaining your data by physically stealing your device, you need to tie that encryption to a passphrase or code that only you know. The previous section explains how to set a passcode

Once your passcode is set your phone is now encrypted. What is crucial is then to **only** back up to your computer or hard drive and never to icloud. That way you retain maximum control of your data.

WARNING: Do not use iCloud to back up your phone. Always back up your content to a hard drive or your own computer. iCloud backups allow Apple and other third parties access to your data. For instance, if they recieve a subpoena to release your personal information to the authorities, there is no guarantee they will be successful guards of your content. That is a lot of trust to give to a corporation. Use your risk assessment to decide what is best for you. At Equality Labs we rarely give our data to corporations for this reason.

Once you've set a passcode, scroll down to the bottom of the Touch ID & Passcode Settings page. You should see a message reading **"Data protection is enabled."** This means that the device's encryption is now tied to your passcode, and most data on your phone will require that code to unlock.



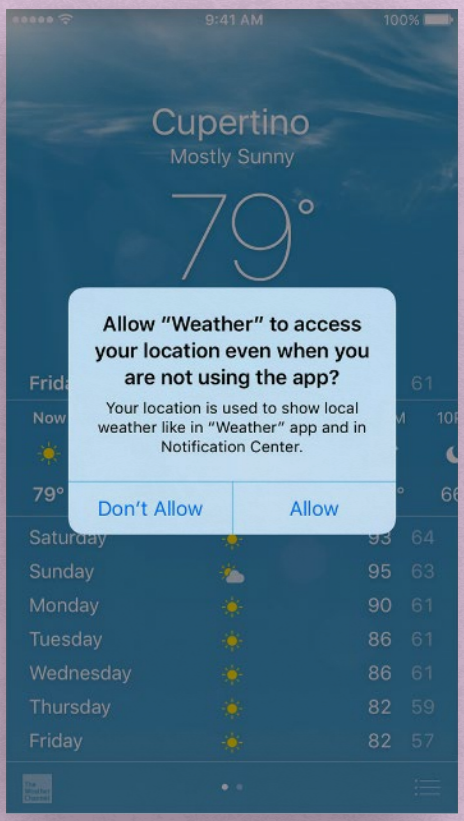
[13] https://ssd.eff.org/en/module/how-encrypt-your-iphone

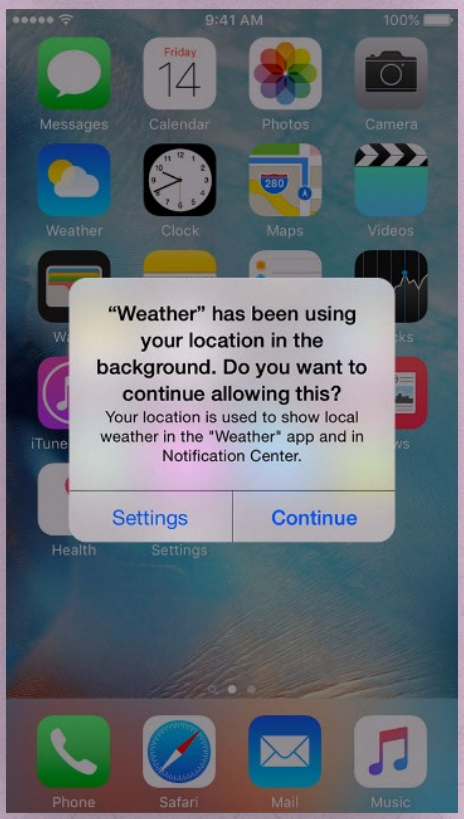
4. TURN OFF LOCATION SERVICES

The first time an app tries to access your location it will ask for your permission, even when it's running in the background. The app's developer may also explain how it uses your location.[14]

Some apps will ask to use your location only while the app is in use. An app is considered "in use" when you are actively using it in the foreground or when it's running idly in the background, which the status bar will indicate.

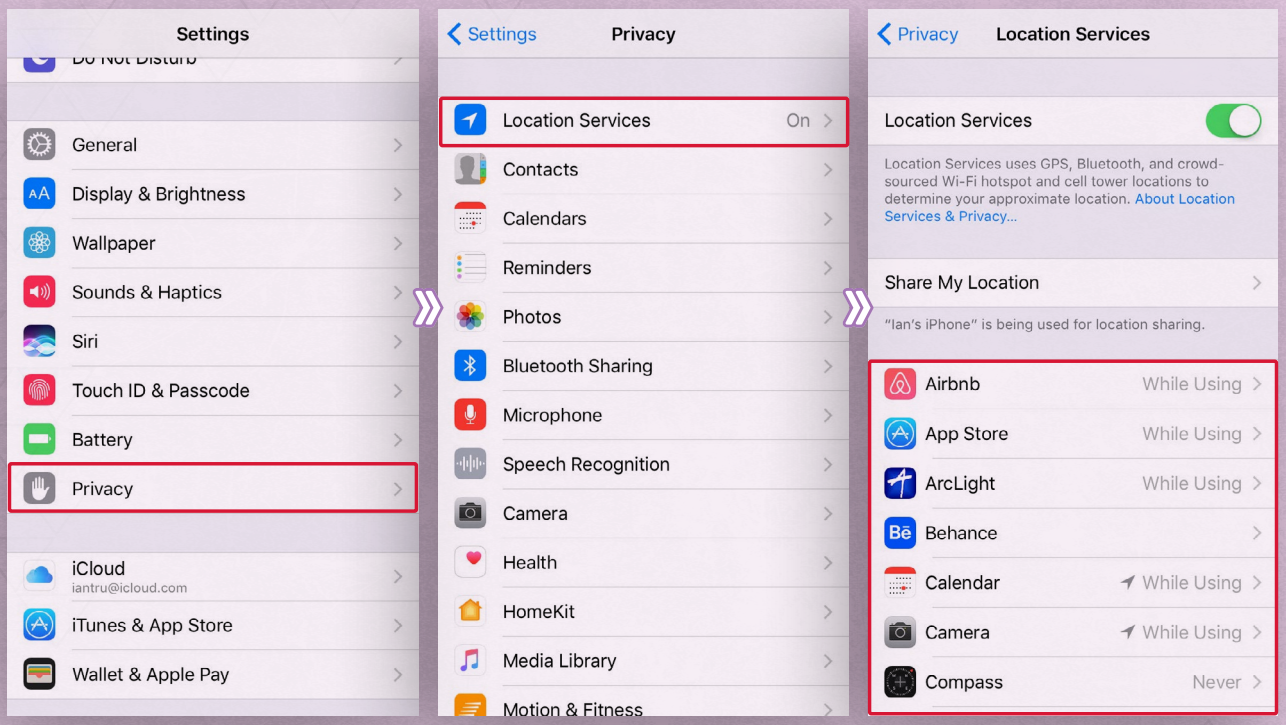
Other apps will ask for access to your location even when they are not in use. Your operating system will remind you which apps have this access with pop-up notifications, triggered when an app uses your location in the background.





[14] https://support.apple.com/en-us/HT203033

- You can control your phone's location settings at **Settings → Privacy → Location Services**. You can turn Location Services on either during the initial Setup Assistant process or later via the Location Services screen. After this, you will be able to control which individual apps and system services have access to your location data.



When Location Services are turned completely off, no apps can use your location in the foreground or background. This may limit applications like Maps and GPS requiring services like Uber or Lyft.

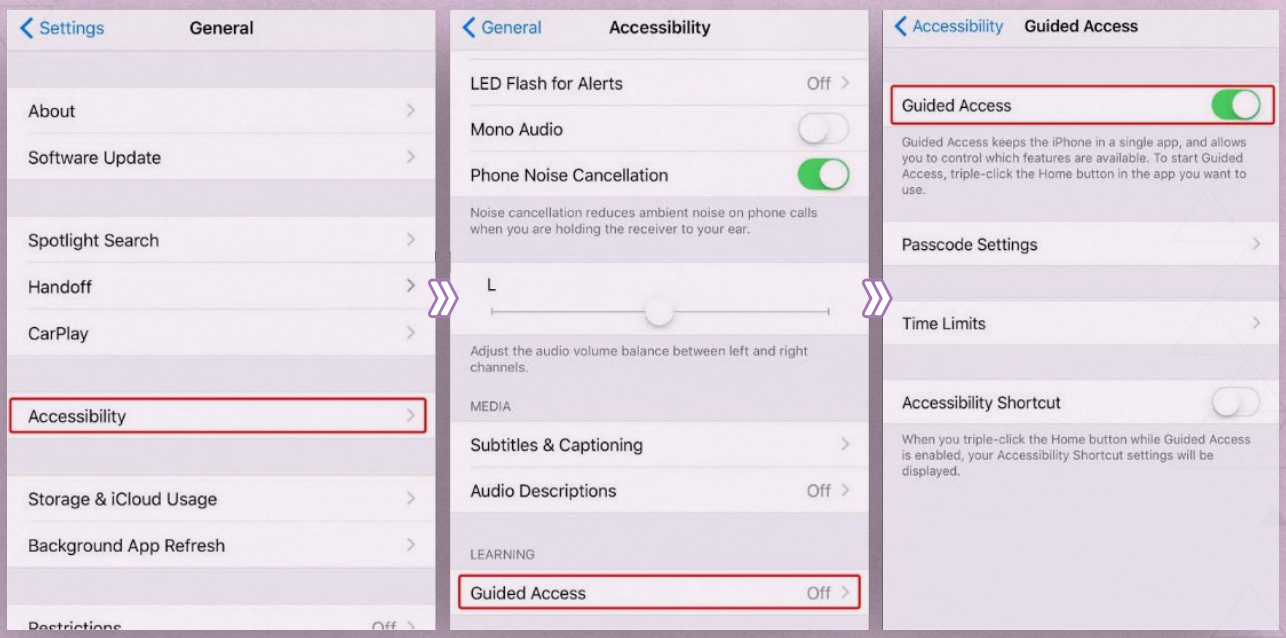
ADDITIONAL SECURITY APPS FOR IPHONE

1. GUIDED ACCESS FOR IPHONES

Apple provides a built-in feature to both hide and lock apps on iPhones.

- Go to Settings and tap **General → Accessibility → Guided Access**. Under Guided Access, toggle Guided Access to ON.

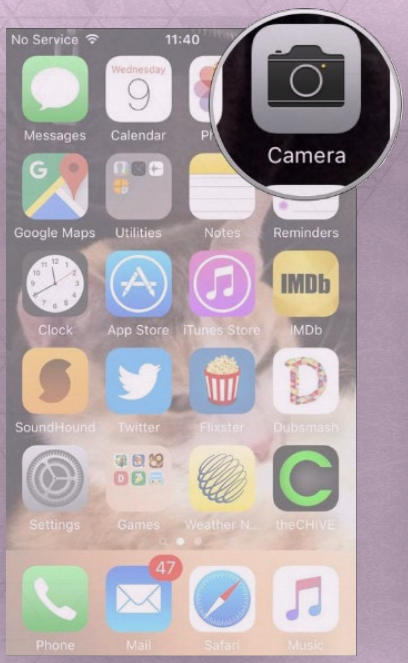
- This will give you an option for—**Passcode Settings**. Now, you can set a Guided Access password.



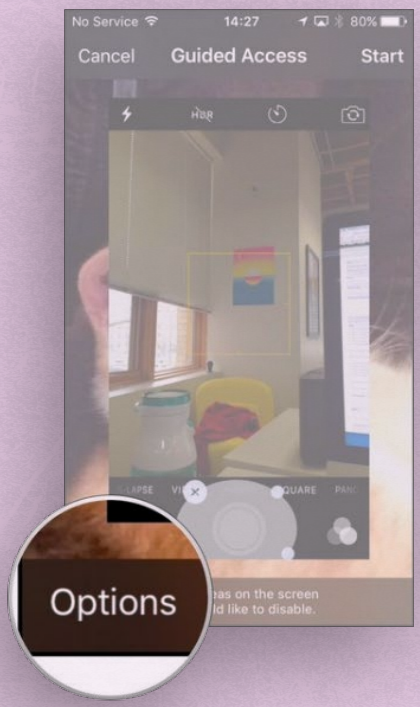
With this, you have successfully enabled the Guided Access feature and can now lock Apps. To do so, open the app you want to lock, for instance, the Camera app.

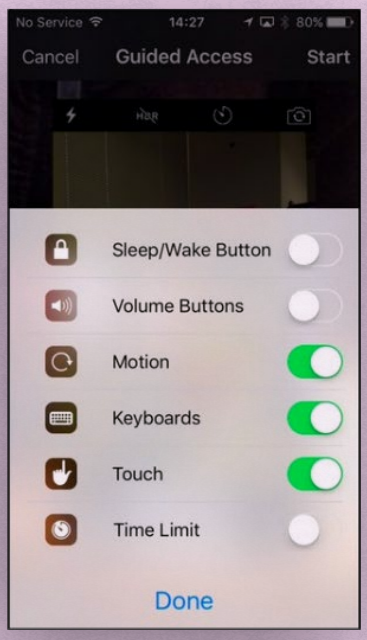
- Next, **triple-click the home button**. This will give you options to restrict features within an app, as shown below. This is the best part of this feature, you may have already seen apps that lock other applications, but the ability to lock specific features within an app is new and different. Simply circle any areas of the screen you would like to make inaccessible.[16]

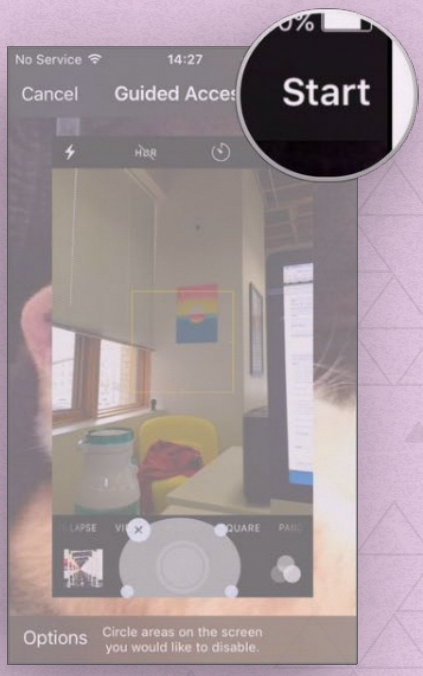
[16] http://www.imore.com/how-use-guided-access-iphone-and-ipad



- Tap on **Options** in the bottom left corner to choose whether you want to grant access to the **sleep/wake** button, **volume** buttons, touch screen, and motion. Tap **Done** to save your selections. Tap on **Start** at the top of the screen to begin Guided Access.







Once Guided Access is enabled, anyone trying to use or leave a specific app will require the passcode. Without the code, he or she will not be able to exit Guided Access.

2. DEALING WITH METADATA ON PHOTOS

Photos we take on all electronic devices can often carry data that can be used to pinpoint our location and gather other information about us.

This information can be intercepted and gathered as part of the surveillance of our movements and habits. These details are often shared through something called **metadata** which is the additional details useful to categorizing, locating, or describing a file. Put simply, metadata refers to data about data.

Many of the files we use and create on our phones have metadata, including emails, text messages, and photos. So one of the ways we can secure our phones is by minimizing the metadata our phones share while we communicate.

The metadata in photographs is known as the **Exchangeable Image File Format,** or **EXIF.** This metadata can reveal much about you, your subject, and where a photo was taken. Metadata embedded in a photo includes the following:

- Key identifying information, such as camera or cell phone user, GPS coordinates, and the time and date the photo was taken
- Camera settings, including static information such as the camera model and make, and information that varies with each image such as orientation (rotation), aperture, shutter speed, focal length, metering mode, and ISO speed information
- A thumbnail preview of the picture on the camera's LCD screen, in file managers, or in photo manipulation software.
- Descriptions of a photographs' content.
- Copyright information.

NOTE: Different versions of iPhones may have different ways to get to the settings described in this section. We describe the general method but do a little searching around the settings areas of your particular version of phone to make sure you achieve the same.

SWITCH OFF LOCATION TAGGING FOR YOUR CAMERA

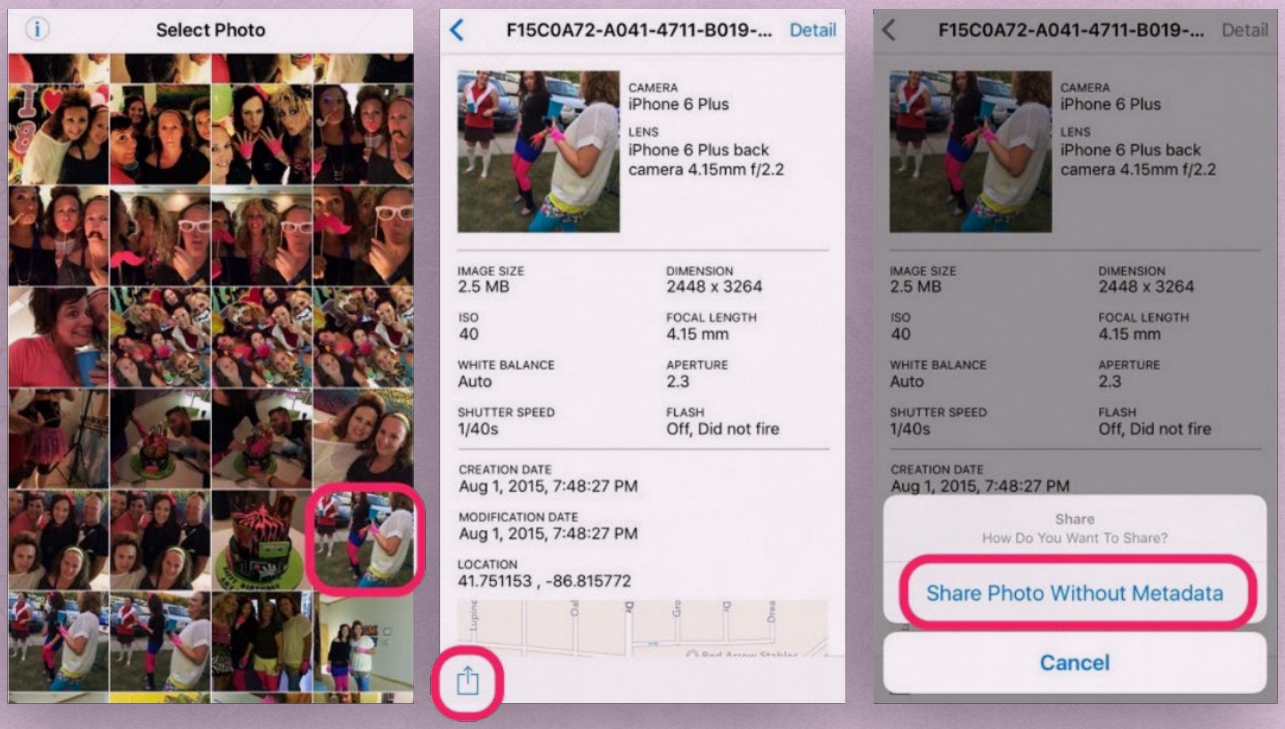
iPhone: Open the Settings app, then tap **Privacy**. Tap **Location Services**, find and tap **Camera** in the list of apps. Under, Allow Loaction Access, select **Never**.

INSTALL A THIRD-PARTY APP FOR SCRUBBING METADATA FROM IMAGES

We recommend using **PixIMet** to remove (“scrub”) existing metadata from photos taken with your phone.

PixlMet for iPhones

This app works the same way. When you choose a photo, it shows you the saved metadata and allows you to share the photo to social media without this data.



NOTE: When removing metadata from a photo that is about to be shared, PixlMet makes a copy of the original photo and only removes metadata from the copy. The original file remains unmodified in your photo library.