WHY DO YOU NEED TO MAKE YOUR IPHONE MORE SECURE?

Your iPhone is securely held together by Face/Touch ID, your passcode and Apple ID password. Since most of us don't use our Apple ID password in a public or crowded space, it's safe, but your iPhone passcode is more vulnerable. If someone has access to your passcode, it can be disastrous.

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

- Change the Apple ID password and lock you out of your own Apple ID
- Change the face ID or touch ID on your iPhone
- Disable Find My iPhone
- Lock you out of other devices signed in with the same Apple ID, like Mac and iPad
- Turn off two-factor authentication
- Access all passwords and Passkeys stored within Password App (IOS 18 onwards)
    - Log in to your banking apps and social media accounts and complete fraud in your name.
- Use Apple Pay and other stored cards on your iPhone name

Even without knowledge of your passcode, if your iPhone is snatched from your hand while unlocked (e.g., during a call), a thief would have access to:

- All your emails configured within the app, notes and photos
- And much, much more…

Over the next few pages, we've listed our top tips to improve the security of your iPhone.

This guide assumes that you are following best practice and keeping your iPhone iOS version to the latest version available.

1. ENABLE STOLEN DEVICE PROTECTION ON IPHONE (IOS 17.3 onwards)

Apple released the 'Stolen Device Protection' feature with iOS 17.3. When enabled, it imposes additional security measures when your iPhone is away from familiar locations, such as home or work.

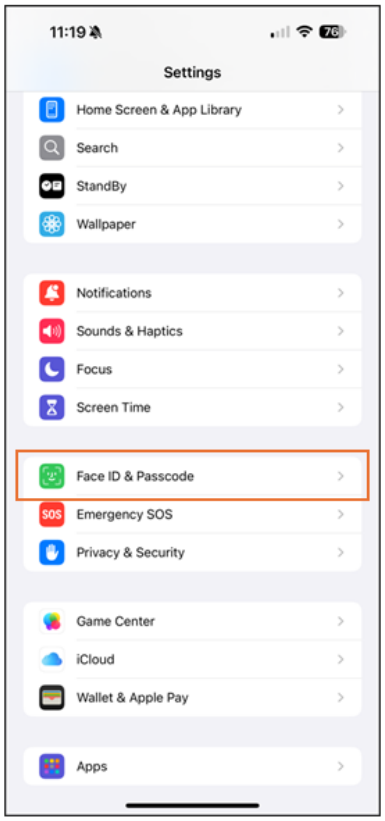
Notable features include the requirement for Face ID or Touch ID authentication for certain actions, such as accessing stored passwords and making critical changes to your Apple ID.

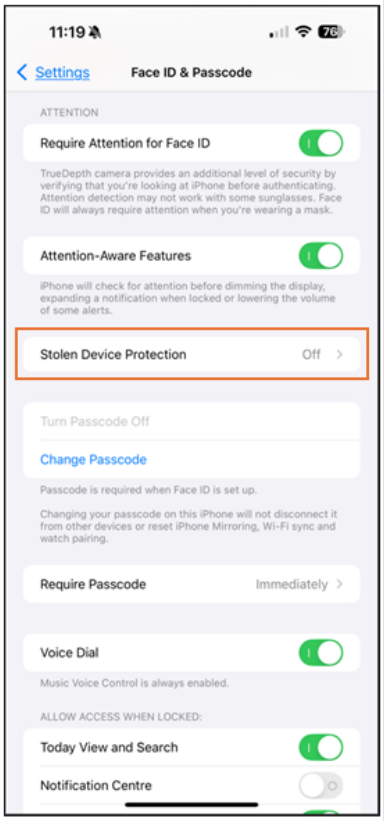
Additionally, a security delay is also implemented for activities like changing your Apple ID password and needs you to wait for an hour and perform biometric authentication twice if you're not in a familiar location.

This security feature is turned off by default; here's how you can enable it:

- **Step 1:** Open the 'Settings' app, scroll down and tap 'Face ID & Passcode' or 'Touch ID & Passcode', enter your passcode when prompted.
- **Step 2:** Scroll down and tap 'Stolen Device Protection' and turn this option on*.

**Note: If you don't see Stolen Device Protection, you may need to set up Face ID or Touch ID first.*

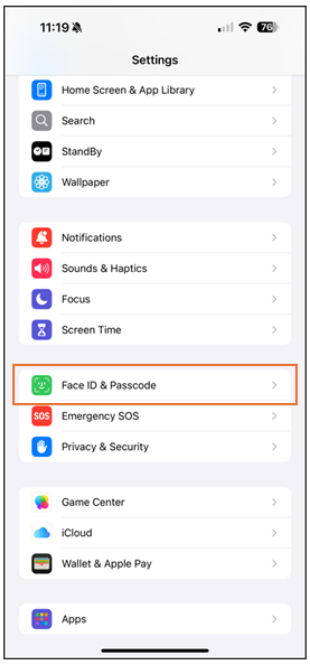


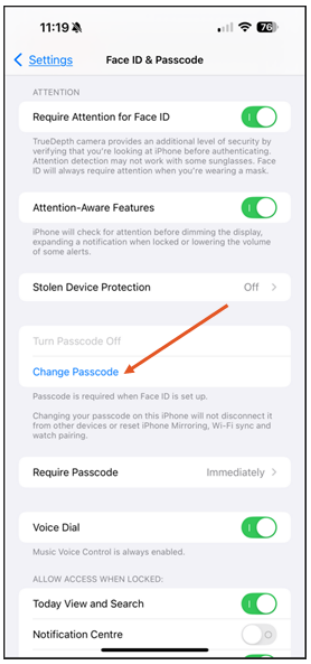


2. USE AN ALPHANUMERIC UNLOCK CODE

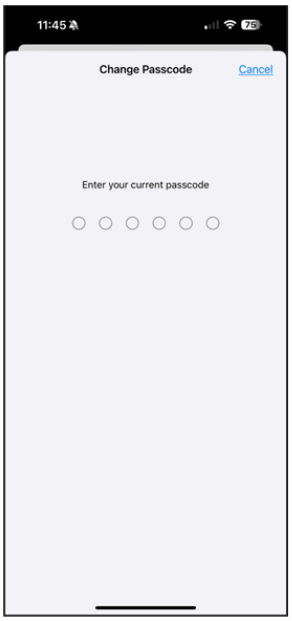
If you've been using a 4-digit numeric passcode to unlock your iPhone, it's time to switch to a more robust option, i.e. an alphanumeric passcode. This is because it is much harder for a potential thief to remember a long passcode than a 4-digit code if they're watching you. Here's how:

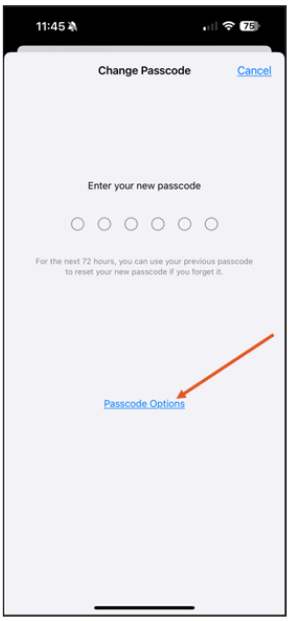
- **Step 1**: Open the 'Settings' app and tap 'Face/Touch ID & Passcode'.
- **Step 2**: Tap 'Change Passcode'.



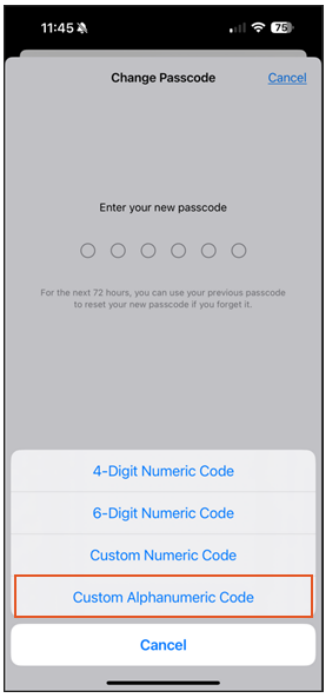


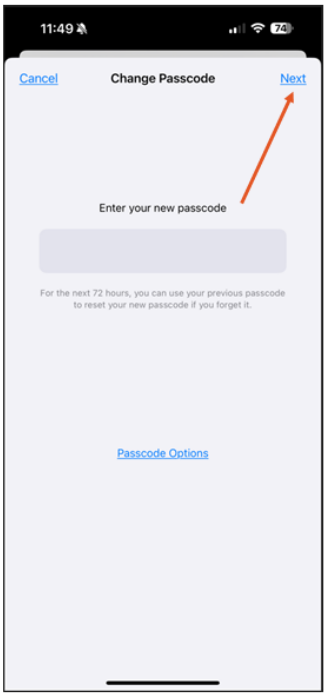
- **Step 3**: Enter your current passcode.
- **Step 4**: Now, tap 'Passcode Options' on the new passcode page.

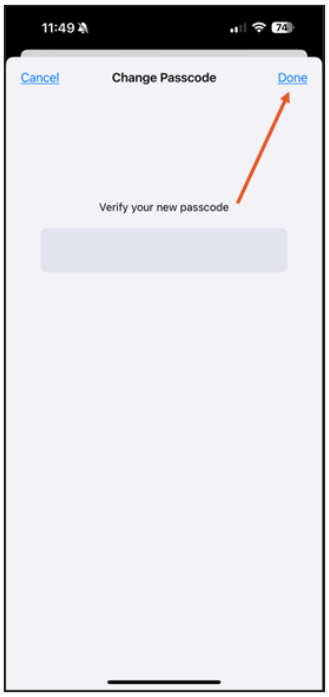




- **Step 5**: Tap ‘Custom Alphanumeric Code’.
- **Step 6**: Type a strong password and tap ‘Next’.
- **Step 7**: Verify your new passcode and tap ‘Done’.

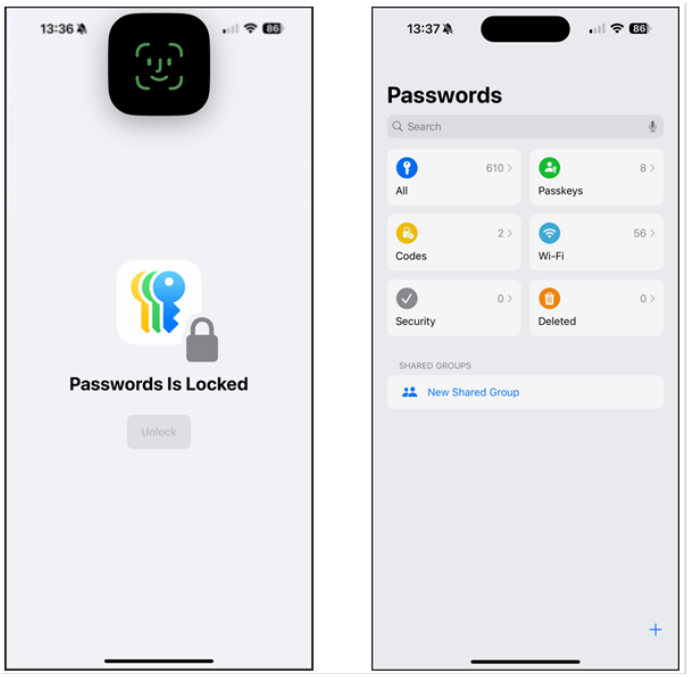






3. PASSWORD APP (IOS 18 ONWARDS)

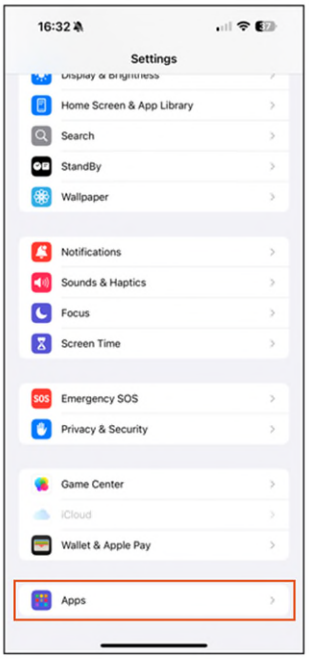
With the introduction of iOS 18, Apple introduced a built-in Password app. This allows users to securely store and manage their passwords, passkeys and verification codes. The app simplifies password management across Apple devices using iCloud Keychain and alerts users to potentially weak or compromised passwords. To gain access the app requires Face/Touch ID to unlock the app.

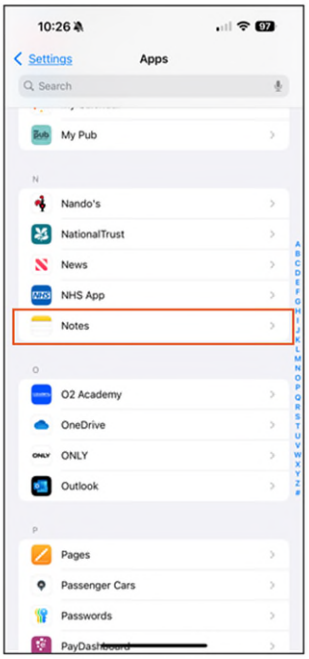


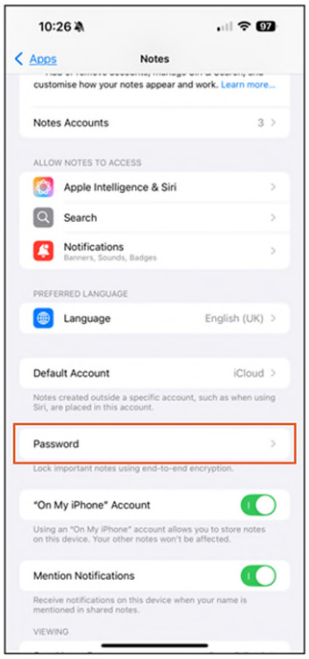
4. NEVER STORE SENSITIVE DETAILS IN NOTES OR PHOTOS

Many of us utilise the Apple Notes app on our iPhones to store various types of data. However, this practice can be misused as the information is readily accessible to a thief who may snatch your unlocked iPhone from your hands, as they don't require a passcode to access these apps. **(Unless you lock with Face/Touch ID – detailed in Section 7 – iOS 18 and above).** It is therefore advisable to delete any PINs or passwords, memorable words/account details, credit/debit card information or sensitive data saved in the Notes app, or pictures of bills/IDs/passports etc. stored in the Photos app.

- **Securing Notes:** The following will only work for Notes from 'iCloud' and 'On My iPhone'. Those imported from other accounts e.g. Gmail/yahoo, etc will not be protected. You should only store sensitive data in these lockable accounts.
  - **Step 1:** Open the 'Settings' app, scroll down and tap 'Apps', then tap 'Notes'.
  - **Step 2:** Tap 'Password', then complete **Step 3** for both 'iCloud' and 'On My iPhone' in turn.

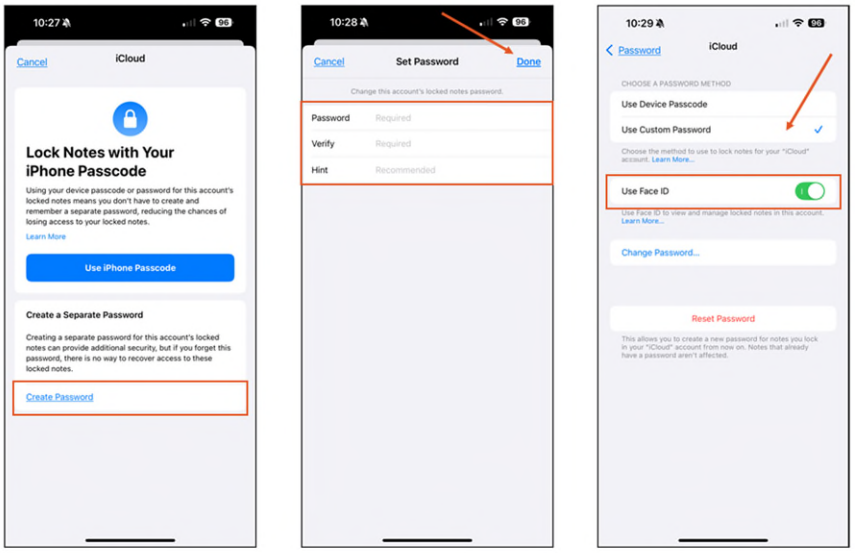




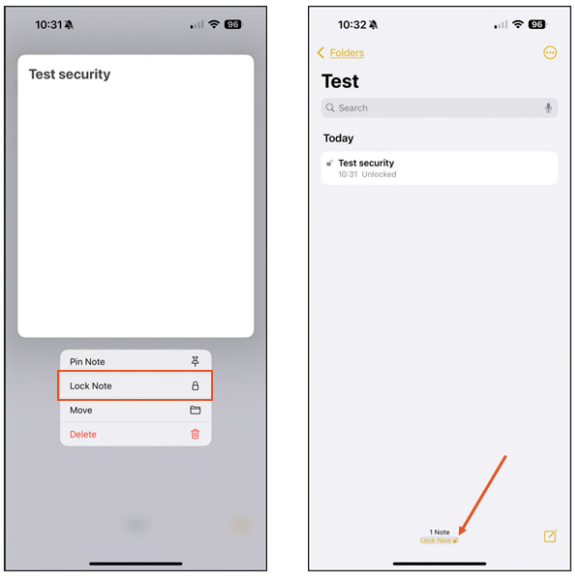


  - **Step 3:** If this is the first time you are setting up a password for Notes, then it will ask you if you wish to use the iPhone Passcode or Create a Separate Password. If you have activated this previously, choose either Use Device Password or Use Custom Password for each account. **Note** a custom password will be more secure than using the device passcode, but it's another password you'll have to remember. It will as you to enter the password twice, along with a password hint.

- **Step 4:** Ensure 'Use Face/Touch ID' is enabled.

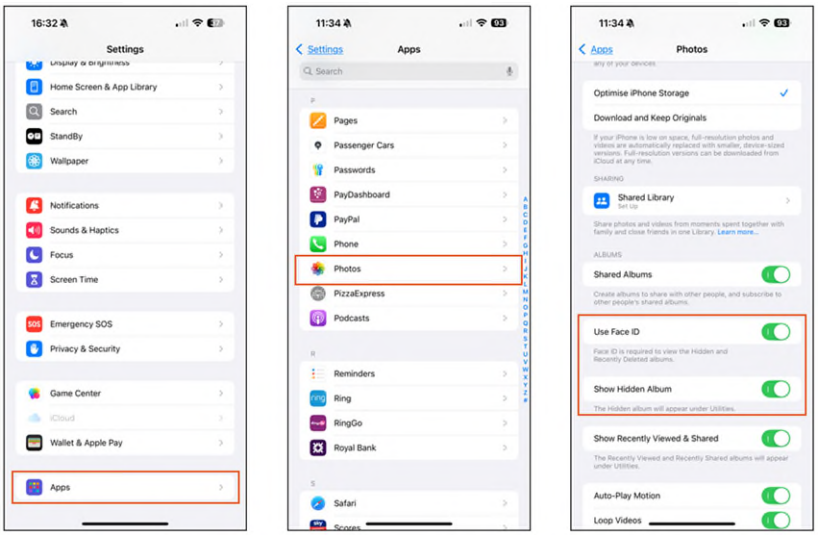


- **Step 5:** Open the 'Notes' app, locate the note you wish to secure, and press and hold that note until the secondary menu appears (bear in mind that the note title will still be visible even when locked, so having a title like "PINS" etc. is not an ideal approach).
- **Step 6:** Select the 'Lock Note' option. Please note that when you utilise Face/Touch ID to enable it, this will unlock all your locked notes. However, they will re-lock if you lock your iPhone, or you can instantly re-secure them using the 'Lock Now' option at the bottom of the Notes List.

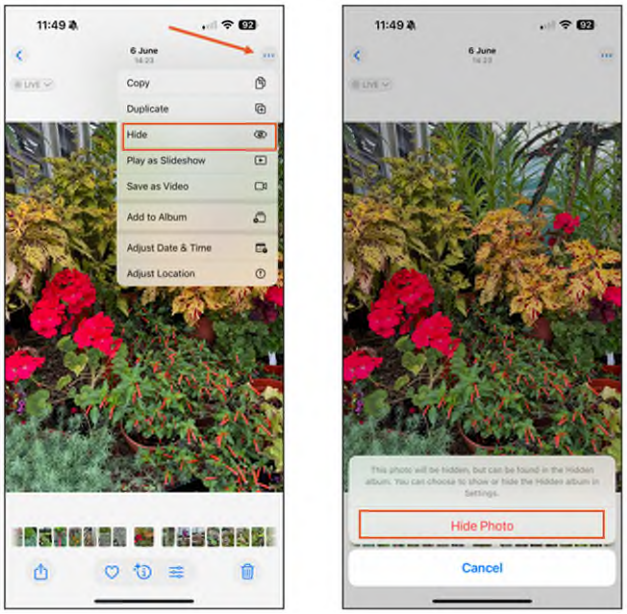


- **Securing Photos**. The Apple Photos app doesn't enable you to lock down individual albums or photos. Instead, there is an optional album called 'Hidden' which is not enabled by default. This folder can be secured with Touch/Face ID, Passcode or Password. Furthermore, you can lock the entire Photos app using the instructions provided in Section 7 by enabling 'Requires Face/Touch ID' – iOS 18 and above.

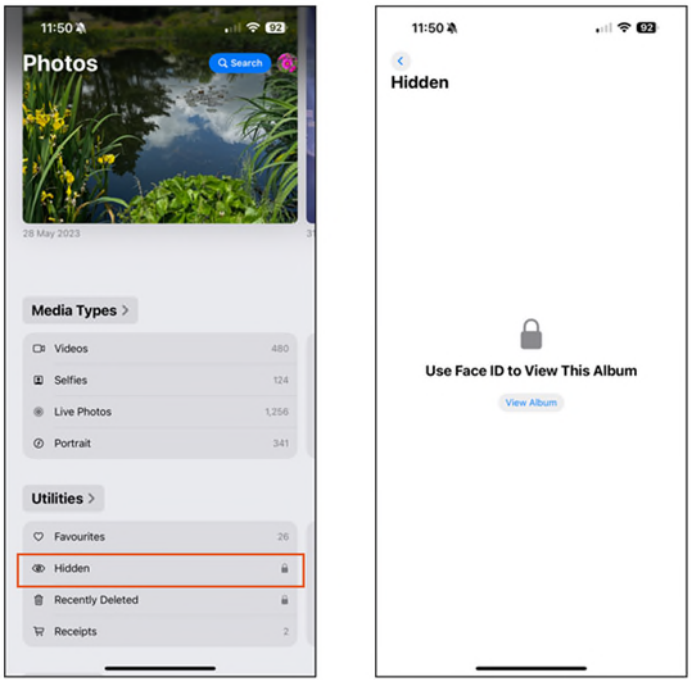
-
  - **Step 1:** Open the ‘Settings’ app, scroll down and tap ‘Apps’, then tap ‘Photos’.
  - **Step 2:** Scroll down to find the ‘Use Face/Touch ID’ and ‘Show Hidden Album’ options and tap toggle them both to on.



  - **Step 3:** To conceal a photo containing sensitive content like your passport, open the photo, tap the ‘three-dot ellipsis’ at the top right, select 'Hide Photo', and confirm to move it to the ‘Hidden’ album (note that you cannot hide entire folders, only individual photos).



- **Step 4:** To view the photos you have hidden, when in the 'Photos' App, scroll down until you find 'Utilities' section and the 'Hidden' option. Note the lock symbol next to it – when you try to open it, you will be asked for 'Face/Touch ID'. The album will automatically lock as soon as you exit it. The same applies to the 'Recently Deleted' album.



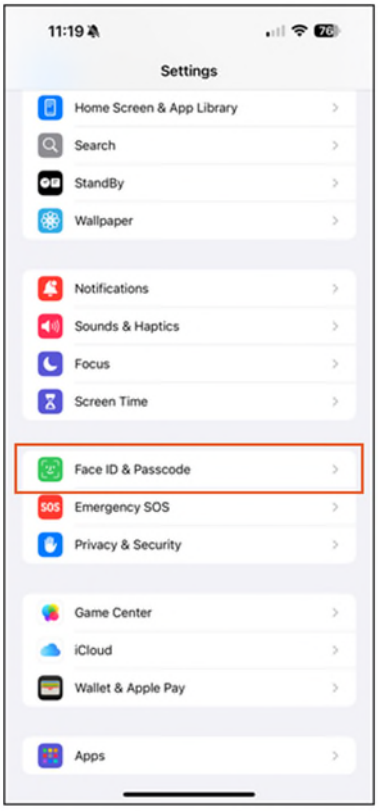
If you must store sensitive data on your iPhone, it is advisable to move notes containing any PINs, passwords, memorable words/account details, credit/debit card information or sensitive data to locked notes in the Notes app. Additionally, transfer pictures of bills, IDs, passports, etc. to the Hidden album in the Photos app. This way, your data will be better protected even if your unlocked iPhone is stolen.

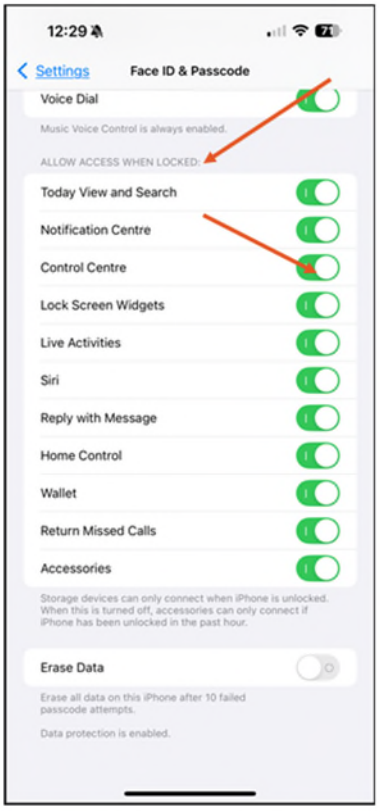
5. DISABLE CONTROL CENTRE ACCESS ON THE LOCK SCREEN

Disabling Control Centre access on the lock screen will stop thieves from activating Airplane Mode. Why is this important? Well, if someone steals your iPhone but doesn't know your passcode, you can use Find My iPhone to track its location from another iOS device. If the thief in question activates Airplane Mode, though, your iPhone can't be tracked using Find My iPhone.

- **Step 1**: Open the 'Settings' app and tap 'Face/Touch ID & Passcode'.
- **Step 2**: Enter your iPhone's passcode.
- **Step 3**: Scroll down to the 'ALLOW ACCESS WHEN LOCKED' menu.
- **Step 4**: Toggle 'Control Centre' off (it's on by default).

(You might want to consider turning others off in this section too)

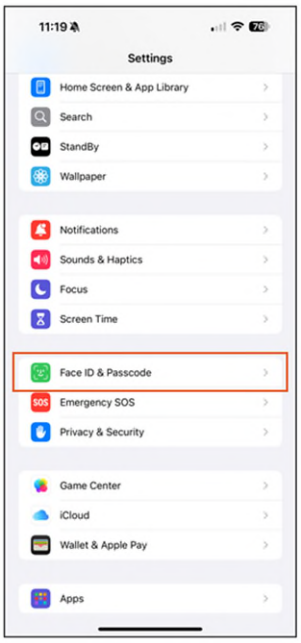


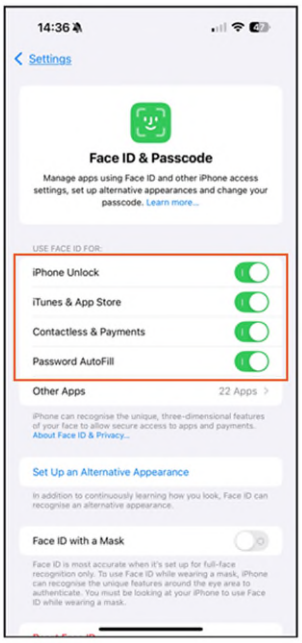


6. PROTECT YOUR ICLOUD KEYCHAIN (AND ANY OTHER PASSWORD MANAGERS)

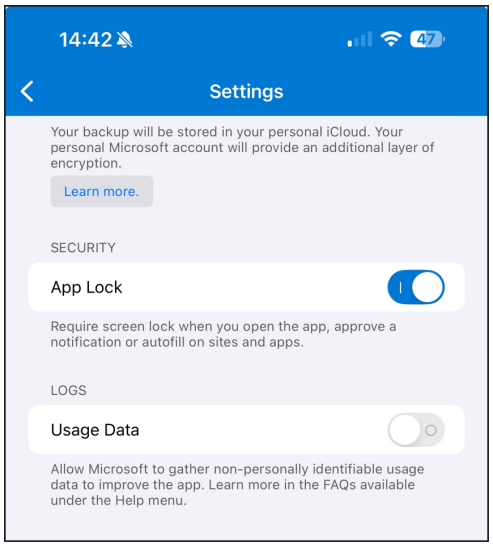
Saving passwords in the iCloud Keychain is convenient, however, it can be easily accessed by anyone who has your iPhone passcode if not protected by biometrics (e.g. Face ID or Touch ID). To turn on biometrics for iCloud Keychain, do the following:

- **Step 1**: Open the 'Settings' app and tap 'Face/Touch ID & Passcode'.
- **Step 2**: Enter your iPhone's passcode.
- **Step 3**: In the 'USE FACE/TOUCH ID FOR' section, turn on all the options if not already toggled on.





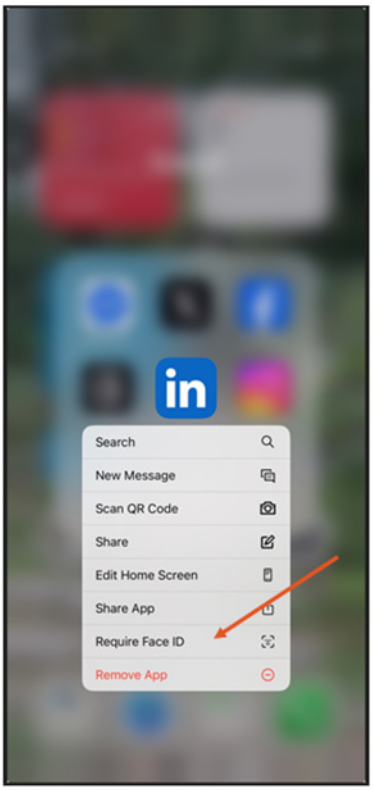
For other password managers, the setting to require biometrics will be found in the settings for that app. For example, in MS Authenticator, it is found under security/app lock.

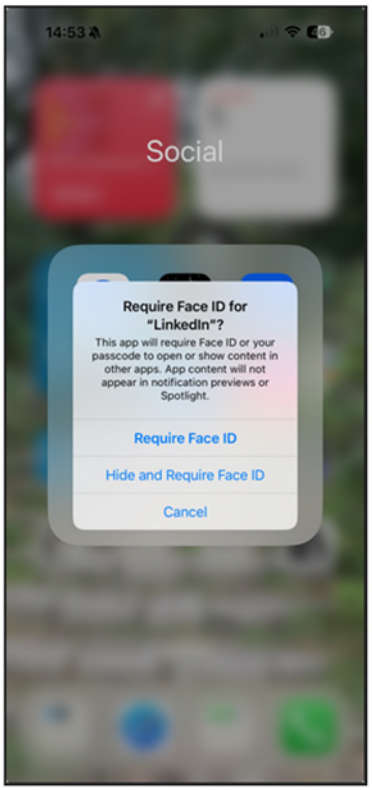


7. LOCK IMPORTANT APPS WITH FACE/TOUCH ID

With the introduction of iOS 18, a new feature was implemented that enables users to lock individual applications. Consequently, Face/Touch ID or passcode authentication is required to gain access to these locked apps, enhancing security and privacy for the user's sensitive data or content within specific applications. To enable this for a specific app, do the following:

- **Step 1**: Press and hold the app you wish to lock, and you will see the following menu.
- **Step 2**: It will then ask if you to select either 'Require Face/Touch ID' or 'Hide and Require Face/Touch ID'. Choose the option that you feel is most suitable from the explanation below:
  - 'Require Face/Touch ID' – App will require Face/Touch ID or passcode to open or show content in other apps. App content will not appear in notification previews or Spotlight.
  - 'Hide and Require Face/Touch ID' – The app will no longer be visible on the iPhone, except in a few places such as Settings. Face/Touch ID or passcode will be required to reveal, open or use Siri with the app.

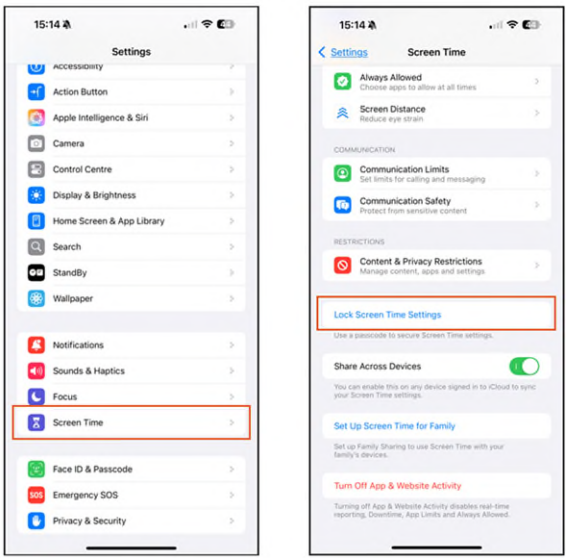




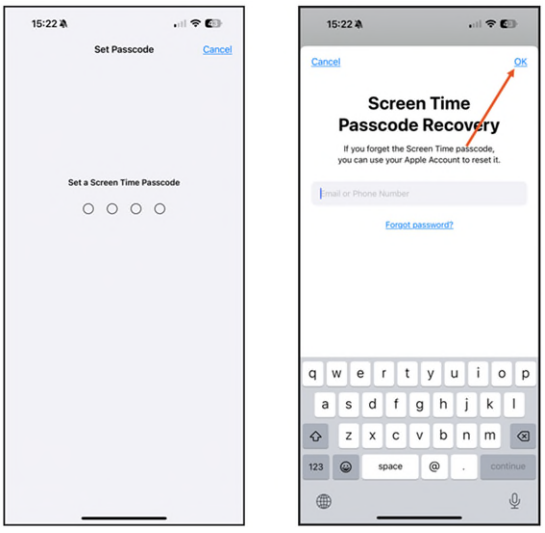
8. TURN OFF PASSCODE & APPLE ID CHANGES

Another thing you can do to prevent others from changing your iPhone passcode and Apple ID password is to restrict this ability by using the screen time feature.

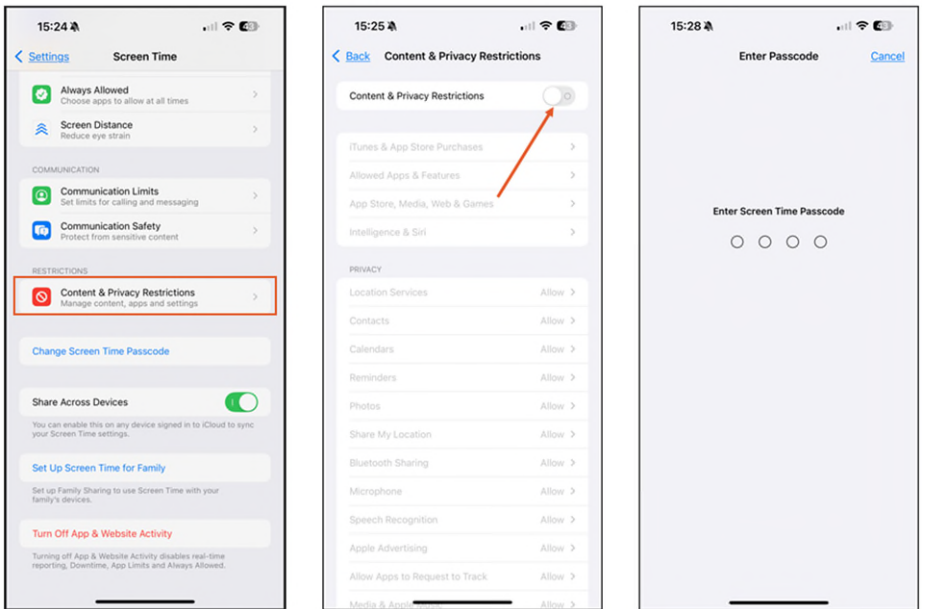
- **Step 1**: Open the 'Settings' and tap 'Screen Time'.
- **Step 2**: Tap 'Lock Screen Time Settings'.



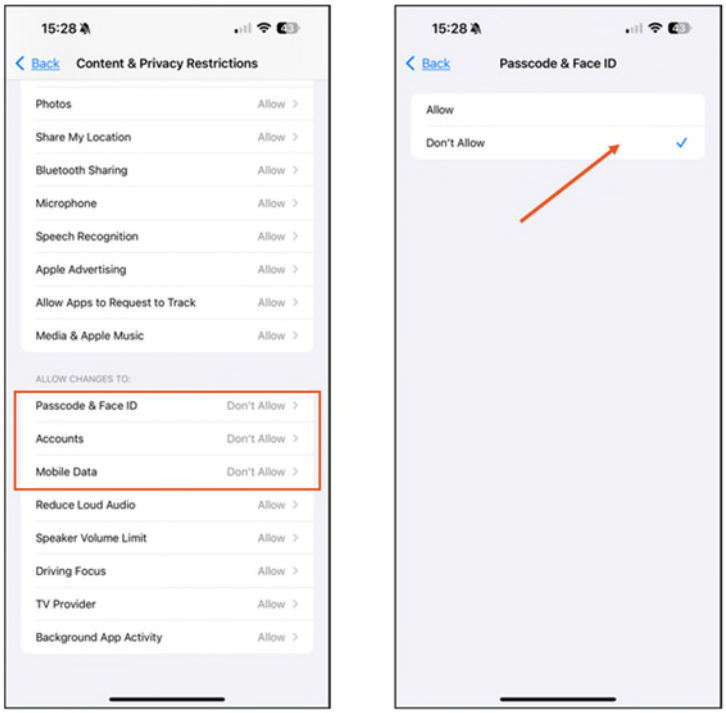
- **Step 3**: Type a unique passcode for screen time.
  - **Note:** Enabling a recovery option in **Step 4** is crucial for passcode recovery; otherwise, a factory reset is required.
  - If you forget the passcode, tap 'Forgot Password' on the 'Change Screen Time Passcode' screen, enter the recovery information to erase the code, then reset it.
- **Step 4**: Type your Apple ID and password on the next screen and tap 'OK'.
  - **Note**: adding Apple ID to screen time will enable you recover the passcode if you forget it.



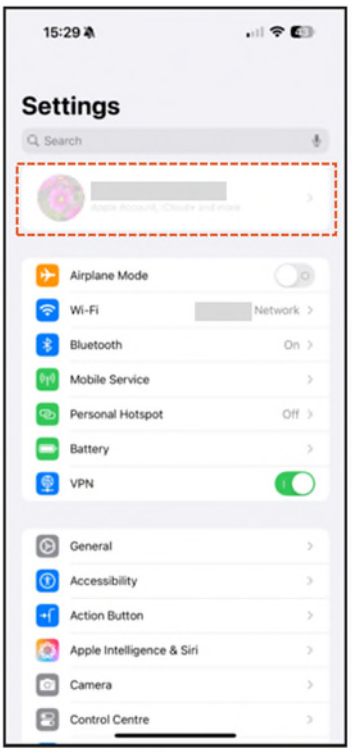
- **Step 5**: Tap 'Content & Privacy Restrictions'.
- **Step 6**: Tap to turn on the toggle for 'Content and Privacy Restrictions'.
- **Step 7**: Enter the screen time passcode.

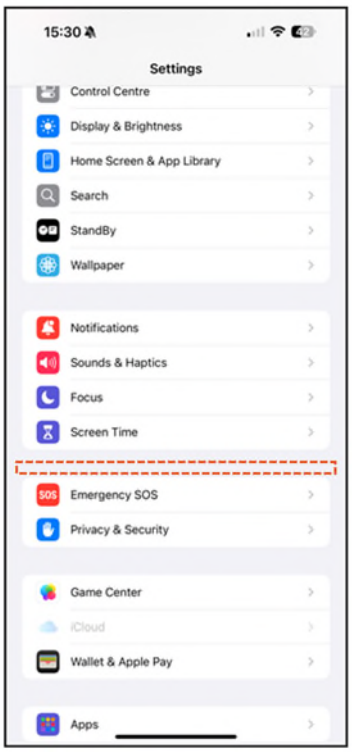


- **Step 8**: Scroll down to the 'ALLOW CHANGES TO' section and set 'Passcode', 'Accounts', and 'Mobile Data' to 'Don't Allow'.



Once done, you will see the Apple ID option greyed out in settings, and the Face/Touch ID & Passcode options disappear from settings. When you want to access those settings, follow the same steps and turn off 'Content & Privacy Restrictions' in screen time.

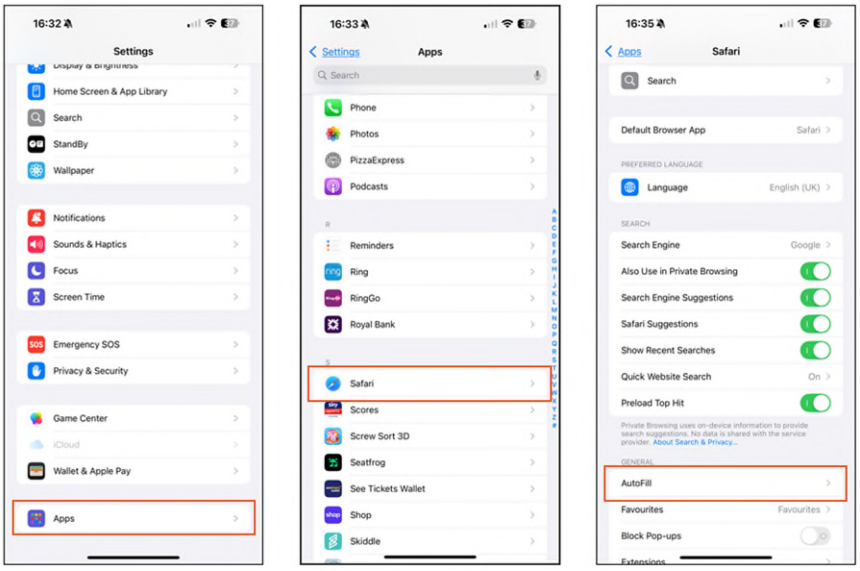




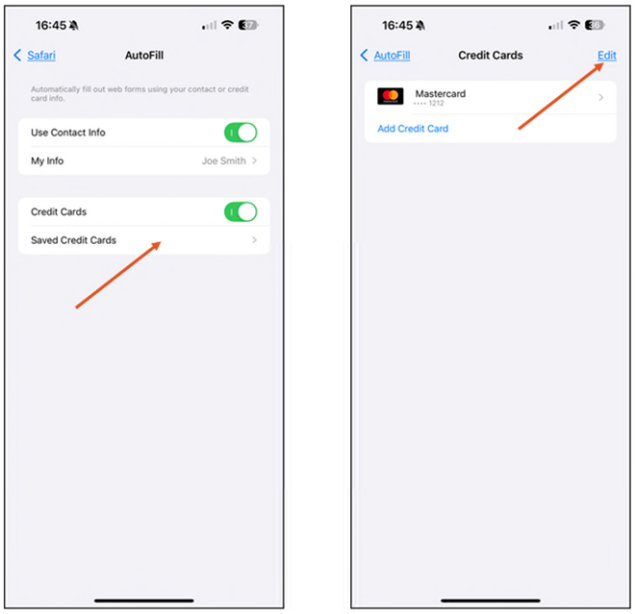
9. REMOVE SAVED CARDS FROM SAFARI

If someone with malicious intent gains access to your iPhone, they can easily make purchases using the card information saved in Safari's Autofill feature. This is because they can also access the one-time password sent to your device. Therefore, it's advisable to remove any saved card details from Safari's Autofill. Note that this is different from removing cards from your Apple Wallet, which has better security measures in place, such as biometric authentication. Follow these steps:

- **Step 1**: Open the 'Settings' app, scroll down and tap 'Apps', then tap 'Safari'.
- **Step 2**: Tap 'Autofill'.



- **Step 3**: Tap 'Saved Credit Cards'.
- **Step 4**: Tap 'Edit'.



- **Step 5**: Select all the cards and tap 'Delete'.