Protecting yourself from phone theft

WEATHERBYS
PRIVATE BANK

Apple devices

Enabling stolen device protection (iOS 17.3.1):

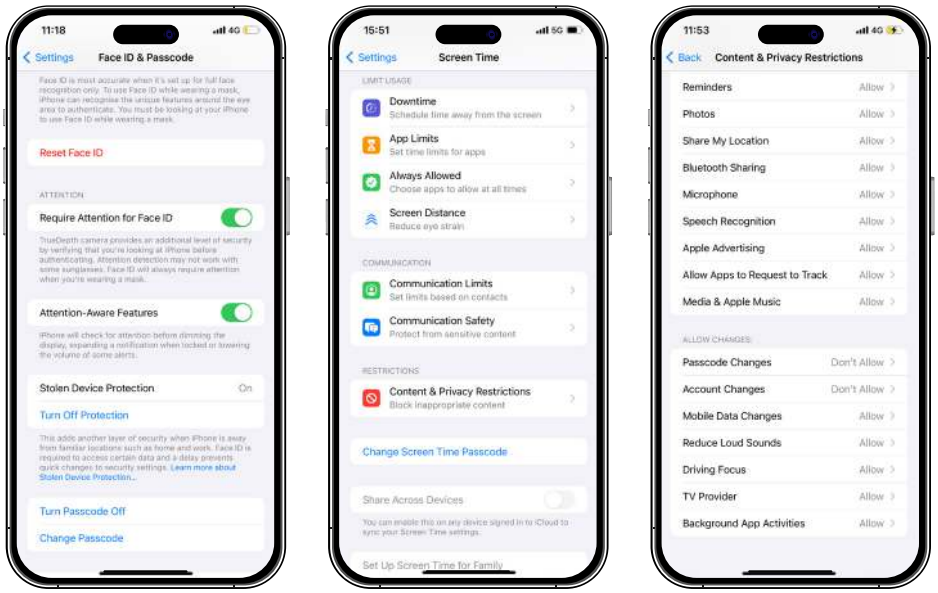
- Ensure your device is updated: Before initiating the process, confirm that your device is running the latest iOS version by going in to Settings > General > Software Update.
- Navigate to Settings: Open the Settings app on your Apple device.
- Access “Face ID & Passcode”: Within Settings, locate and select “Face ID & Passcode”.
- Enter your passcode: Input the passcode used to unlock your device.
- Locate “Stolen Device Protection”: Scroll down within the “Face ID & Passcode” settings to find the option for “Stolen Device Protection”.
- Enable “Stolen Device Protection”: Toggle the switch to “Turn On” to activate this feature. This adds an extra layer of security to prevent unauthorised access.

Restricting account and passcode changes:

- Access “Screen Time”: Return to the main Settings screen and tap on “Screen Time”.
- Navigate to “Lock Screen Time Settings”: Within Screen Time, tap on “Lock Screen Time Settings”.
- Set up a separate 4-digit passcode: Create a unique 4-digit passcode (this must be different from your device passcode) and enter it twice when prompted.
- Log in to your Apple ID: Enter your Apple ID credentials. This is crucial for recovering the Screen Time passcode if forgotten.
- Enable “Content & Privacy Restrictions”: After setting up Screen Time passcode, click on “Content & Privacy Restrictions”.
- Restrict “Passcode Changes”: Under “Passcode Changes”, enter the 4-digit passcode you created earlier and change it to “**Don’t Allow**”.
- Restrict “Account Changes”: Navigate to “Account Changes” and change it to “**Don’t Allow**”.

By restricting account and passcode changes, you add an extra layer of defence against unauthorised alterations to your device. In the event of a stolen phone, these measures prevent fraudsters from easily changing critical settings or accessing sensitive information, enhancing the overall security of your iPhone and reducing the risk of unauthorised transactions or account breaches.

Your settings should now look like the below:



Find My app:

1. Activation and Setup: Ensure that "Find My" is activated on your Apple device. You can enable it in the device settings under "Find My" or "iCloud".
2. Accessing from Another Device: In the event of a lost or stolen device, you can access the "Find My" service from another device. You can do this directly through the iCloud website or via another Apple device.
3. Using "Find My" app via iCloud Website: Log in to the iCloud website (**https://www.icloud.com/find**) from any web browser.
4. Using "Find My" on another Apple Device: Open the "Find My" app on another Apple device, such as an iPhone or iPad.
5. Remote Actions: You can perform various actions remotely:
    - Play Sound: Helps you locate your device if it is nearby by playing a sound, even if it is on silent.
    - Secure Device (Lock): Enables you to remotely lock your device with a new passcode and displays a custom message on the lock screen.
    - Erase Device: Allows you to erase all data on your device if recovery is not possible.

It is essential to note that for "Find My" to be effective, your device must be turned on, connected to the internet and have location services enabled. Additionally, your Apple ID must be signed in on the device. This feature provides powerful tools to secure your data and significantly increases the chances of recovering a lost or stolen Apple device.

Immediate actions if your phone is stolen:

- Locate Your Device: Access the "Find My" app on another Apple device or use the iCloud website to track the stolen phone.
- Lock Your Device: Utilise the "Find My" app to remotely activate the "Lost Mode", allowing you to lock your device with a passcode and display a custom message on the lock screen.
- Erase Data: If necessary, use the "Find My" app to initiate a full erase of your device, ensuring your data is protected.
- Report to Authorities: File a police report and provide them with the necessary information, including the tracked location.

Android devices

Protective measures:

- Install a Device Locator App: Utilise reputable apps like “Find My Device” for Android or other third-party security apps that allow you to track your phone’s location in case of theft.
- Set up Screen Lock: Enable a secure screen lock method such as passcode, password or pattern to prevent unauthorised access. If using a passcode, please ensure that it differs from any other passcodes you may currently use.
- Enable Biometric Authentication: If your Android device supports it, activate finger or facial recognition for an additional layer of security.
- Activate “Find My Device”: On Android devices, you can enable the “Find My Device” feature in your Google Account settings. This helps locate, lock or erase your device remotely.
- Regularly Update Software: Ensure your Android device is running the latest software updates to benefit from improved security features.

Find my device app:

- Activation and Setup: Ensure that “Find My Device” is activated on your Android phone. You can enable it in the device settings under “Google” or “Security & Location”.
- Accessing from Another Device: In the event of a lost or stolen phone, you can access “Find My Device” service from another device, such as a computer or another Android device.
- Using “Find My Device” app via Website: Open a web browser and go to the “Find My Device” website (**https://www.google.com/android/find**).
- Using “Find My Device” on Another Android Device: Open the “Find My Device” app on another Android device, such as a phone or tablet.
- Device Location: The service will display the last known location of your device on a map, along with additional options.
- Remote Actions: You can perform various actions remotely:
    - Play Sound: Helps you locate your device if it is nearby by playing a sound, even if it is on silent.
    - Secure Device (Lock): Enables you to remotely lock your device with a new password.
    - Erase Device: Allows you to erase all data on your device if recovery is not possible.

It is important to note that for “Find My Device” to work, your device must be connected to the internet and have location services enabled. Additionally, your Google Account must be signed in on the device. This feature provides valuable tools to protect your data and increase the chances of recovering a lost or stolen Android phone.

Immediate actions if your phone is stolen:

- Locate Your Device: Use “Find My Device” to track the location of your stolen phone.
- Lock Your Device: Remotely lock your device via the tracking app to prevent unauthorised access.
- Erase Data: If necessary, you can remotely erase your device to protect sensitive information.
- Report to Authorities: File a police report and provide them with the necessary information, including the tracked location.

This document is for guidance only. For any technical advice, please contact your mobile phone provider.

WEATHERBYS PRIVATE BANK

Sanders Road Wellingborough Northamptonshire NN8 4BX

+ 44 (0)1933 543 600 privatebank@weatherbys.bank www.weatherbys.bank

February 2024