J.P.Morgan

CYBER SAFETY

Securing your mobile devices

Your mobile device, which has made life so much more convenient, now uses Artificial Intelligence (AI) to personalize your experience and streamline daily tasks. However, AI also enables your device to track who you are, where you have been, and information about your friends, family, and contacts. This advanced technology can make you and your device a prime target for hackers seeking valuable data. Here are some easy steps to keep your information more secure.

Note: Menu navigation in this guide may vary based on your mobile carrier and software version.

Mobile device safety guidelines

- **Set a passcode on your mobile device** as one of your first lines of defense. Use a 6-digit lock code and enable biometrics (fingerprint or facial recognition) on your mobile device. Avoid using a swipe pattern that can be easily guessed or shoulder surfed. Guard your mobile device code as you would a bank or credit card PIN code
- **Review the apps on your phone** and what type of data they collect and share with others. Stop your phone and apps from tracking your location when they are not in use

  Tip: Always download apps from official stores (App Store or Google Play), and be cautious about granting app permissions.
- **Install a mobile security app and/or anti-virus** from a reputable provider on your mobile devices
- **Enable tracking, controlling and wiping** of your mobile device when not in your possession, so you can remotely erase all data on your device if it is lost or stolen
- **Ensure your privacy settings are on** and set at a level that keeps your information more private. Visit www.apple.com/privacy, www.samsung.com/privacy, or www.google.com/privacy to learn more

Instructions for popular mobile devices on:

- Locking your device
- Limiting information appearing on your screen
- Protecting your data

SECURING YOUR IPHONE (FACE ID) Operating System: iOS 26

Limit your potential exposure

1. Lock your device

Setting a passcode on your mobile device is one of your first lines of defense in keeping your information private, particularly in the event your device is lost or stolen.

- Navigate to **Settings** > **Face ID & Passcode** > **Turn Passcode ON** > Enter a 6-digit passcode

Use **Face ID** if you prefer to unlock your iOS device with your face:

- Navigate to **Settings** > **Face ID & Passcode** > **Set Up Face ID** > Switch ON: **iPhone Unlock**

2. Limit information appearing on your lock screen and access to your device

Prevent important information about you and/or your contacts from appearing on your locked device:

- Navigate to **Settings** > **Face ID & Passcode** > Enter Passcode > **Allow Access When Locked** section > Switch OFF: **Today View and Search, Notification Center, Control Center, Lock Screen Widgets, Live Activities, Siri, Reply with Message, Home Control, Wallet, Return Missed Calls,** and **Workout Health Data**
- Navigate to **Settings** > **Siri > Talk to Siri** > Switch OFF

Is your phone broadcasting your name?

- Navigate to **Settings** > Select your **Apple Account** > **Personal Information** > **Name** > **Rename**

Disable wireless technologies when not in use:

- Wi-Fi:
  Settings > **Wi-Fi** > **Ask to Join Networks** > Switch OFF
- Bluetooth:
  Settings > **Bluetooth** > Switch OFF
- AirDrop:
  Settings > **General** > **AirDrop** > *Suggestion: Switch to "Receiving Off" or "Contacts Only"*

Ensure your device is not connected to unfamiliar Wi-Fi networks:

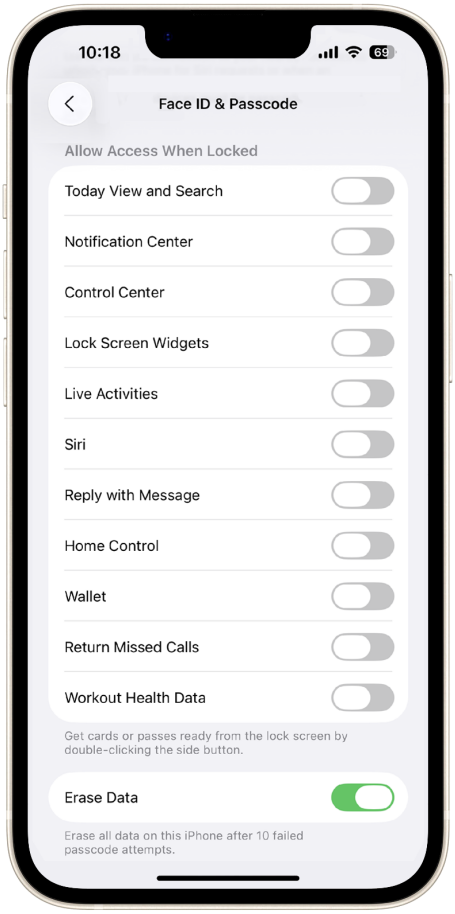
- Navigate to **Passwords** app > **Wi-Fi** > Review all listed networks, and if you see any unfamiliar ones select **Forget This Network**

3. Protect your data if your phone is lost or stolen

Set your phone to automatically erase all of your data after 10 incorrect password attempts:

- Navigate to **Settings** > **Face ID & Passcode** > Enter Passcode > Switch ON: **Erase Data**

Note: Regularly back up your device to iCloud or your computer, to ensure you can reinstall your data, apps and settings upon recovery.



4. Disable tracking of your device

By default, iOS tracks your device's most frequently visited locations. Disabling this feature ensures that information could never end up in the wrong hands:

- Navigate to **Settings** > **Privacy & Security** > **Location Services** > **System Services** > **Significant Locations & Routes** > **Clear History** > Switch OFF

  Your device will ask you to use **Face ID** or the passcode to see **Significant Locations & Routes**.

5. Limit data and location tracking

Application tracking

Some applications need your current location in order to function. Stop them from tracking your location when you're not using them:

- Navigate to **Settings** > **Privacy & Security** > **Location Services** > *Change access for each app from Always to either* **Never** *or* **While Using the App**

  Review the **Precise Location** section for each app and decide which apps may need this feature (e.g., ridesharing, travel apps) or just your approximate location).

Tracking

Limit the ability for apps to use information about you from other apps on your device.

- Navigate to **Settings** > **Privacy & Security** > **Tracking** > Switch OFF: **Allow Apps to Request to Track**

App access

- Navigate to **Settings** > **Privacy & Security**. Review which features of your phone an app has access to. Moderate which apps have access to data like Contacts, Calendars, Photos and Health.

Analytics & Improvements

A feature that collects anonymous data about your device and its performance to help Apple improve its products and services.

- Navigate to **Settings** > **Privacy & Security** > **Analytics & Improvements** > Review all options and consider switching these options OFF

Apple Advertising

Limit advertisers from building a personal profile about you:

- Navigate to **Settings** > **Privacy & Security** > **Apple Advertising** > Switch OFF: **Personalized Ads**

6. Find your device if it's misplaced, lost or stolen

Locate and maintain control of your iPhone, even if it's not in your possession, by:

- Changing your passcode
- Preventing it from being reactivated with another phone number
- Erasing all of your data

- Navigate to **Settings** > **Apple ID profile** > **Find My** > **Find My iPhone** > **Switch ON: Find My iPhone**, **Find My Network**, and **Send Last Location**

  Consider using an additional feature, **Stolen Device Protection**. Stolen Device Protection adds a layer of security when your iPhone is away from familiar locations, such as home or work, and helps protect your accounts and personal information in case your iPhone is ever stolen.

- Navigate to **Settings** > **Privacy & Security** > **Stolen Device Protection** > Switch ON > Review **Require Security Delay** and choose the option best suited to your needs

  Strongly consider installing a reputable anti-virus app from the App Store. It can provide advanced theft alerts and monitor your device for potentially malicious activity.

7. Password protect app purchases

Control what's downloaded or purchased on your device through the App Store by requiring your password to be entered before a transaction can be completed:

- Navigate to **Settings** > **Screen Time** > **Content & Privacy Restrictions** > **iTunes & App Store Purchases** > Select **Always Require**

8. Phone Screening

This option makes unknown callers state why they are calling, and provides you with a transcript before your iPhone rings, allowing you to decide whether to answer the call.

- Navigate to **Settings** > **Apps** > **Phone**, scroll down, and under the **Screen Unknown Callers** section, select **Ask Reason for Calling**

9. Apple Intelligence & Siri

A personal intelligence system integrated into your iPhone, apps, and Siri.

- Navigate to **Settings** > **Apple Intelligence & Siri** > **Apple Intelligence** > Consider switching this feature OFF
- Scroll down to the **Extensions** section > Tap on an extension to review access settings
- Consider disabling **Setup Prompts** feature
- Review other features and adjust based on your level of comfort

SECURING YOUR IPHONE (TOUCH ID) AND IPAD — Operating System: iOS 26

Limit your potential exposure

1. Lock your device

Setting a passcode on your mobile device is one of your first lines of defense in keeping your information private, particularly in the event your device is lost or stolen.

- Navigate to **Settings** > **Touch ID & Passcode** > **Turn Passcode ON** > Enter a 6-digit passcode

Use **Touch ID** if you prefer to unlock your iOS device with your fingerprint:

- Navigate to **Settings** > **Touch ID & Passcode** > **Add a fingerprint** > Switch ON: **iPhone Unlock**

2. Limit information appearing on your lock screen and access to your device

Prevent information about you and/or your contacts from appearing on your locked device:

- Navigate to **Settings** > **Touch ID & Passcode** > Enter Passcode > *Allow Access When Locked* section > Switch OFF: **Today View and Search, Notification Center, Control Center, Lock Screen Widgets, Live Activities, Siri, Reply with Message, Home Control, Wallet, Return Missed Calls, and Workout Health Data**
- Navigate to **Settings** > **Siri > Talk to Siri** > Switch OFF

Is your phone broadcasting your name?

- Navigate to **Settings** > Select your **Apple Account** > **Personal Information** > **Name** > **Rename** Disable wireless technologies when not in use:
- Wi-Fi:
  Settings > **Wi-Fi** > **Ask to Join Networks** > Switch OFF
- Bluetooth:
  Settings > **Bluetooth** > Switch OFF
- AirDrop:
  Settings > **General** > **AirDrop** > *Suggestion: Switch to "Receiving Off" or "Contacts Only"*

Ensure your device is not connected to unfamiliar Wi-Fi networks:

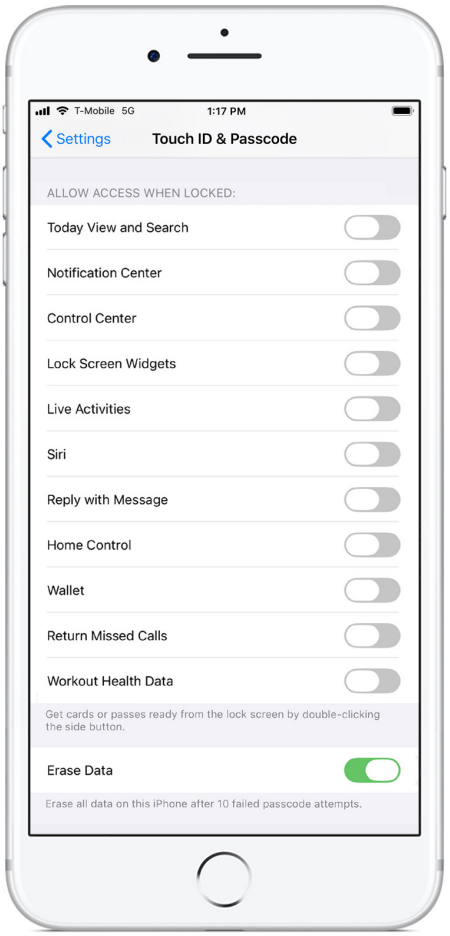
- Navigate to **Passwords** app > **Wi-Fi** > Review all listed networks, and if you see any unfamiliar ones select **Forget This Network**

3. Protect your data if your phone is lost or stolen

Set your phone to automatically erase all of your data after 10 incorrect password attempts:

- Navigate to **Settings** > **Touch ID & Passcode** > Enter Passcode > Switch ON: **Erase Data**

Note: Regularly back up your device to iCloud or your computer, to ensure you can reinstall your data, apps and settings upon recovery.



4. Disable tracking of your device

By default, iOS tracks your device's most frequently visited locations. Disabling this feature ensures that information could never end up in the wrong hands:

- Navigate to **Settings** > **Privacy & Security** > **Location Services** > **System Services** > **Significant Locations & Routes** > **Clear History** > Switch OFF

  Your device will ask you to use TouchID or the passcode to see **Significant Locations & Routes**.

5. Limit data and location tracking

Application tracking

Some applications need your current location in order to function. Stop them from tracking your location when you're not using them:

- Navigate to **Settings** > **Privacy & Security** > **Location Services** > *Change access for each app from Always to either* **Never** *or* **While Using the App**

  Review the **Precise Location** section for each app and decide which apps may need this feature (e.g., ridesharing, travel apps) or just your approximate location.

Tracking

Limit the ability for apps to use information about you from other apps on your device.

- Navigate to **Settings** > **Privacy & Security** > **Tracking** > Switch OFF: **Allow Apps to Request to Track**

App access

- Navigate to **Settings** > **Privacy & Security**. Review which features of your phone an app has access to. Moderate which apps have access to data such as Contacts, Calendars, Photos and Health.

Analytics & Improvements

A feature that collects anonymous data about your device and its performance to help Apple improve its products and services.

- Navigate to **Settings** > **Privacy & Security** > **Analytics & Improvements** > Review all options and consider switching these options OFF

Apple Advertising

Limit advertisers from building a personal profile about you:

- Navigate to **Settings** > **Privacy & Security** > **Apple Advertising** > Switch OFF: **Personalized Ads**

6. Find your device if it's misplaced, lost or stolen

Locate and maintain control of your iPhone or iPad, even if it's not in your possession, by:

- Changing your passcode
- Preventing it from being reactivated with another phone number
- Erasing all of your data

- Navigate to **Settings** > **Apple ID profile** > **Find My** > **Find My iPhone** (or **iPad**) > Switch ON: **Find My iPhone** (or **iPad**), **Find My Network**, and **Send Last Location**

  Consider using an additional feature, **Stolen Device Protection**. Stolen Device Protection adds a layer of security when your iPhone is away from familiar locations, such as home or work, and helps protect your accounts and personal information in case your iPhone is ever stolen.

- Navigate to **Settings** > **Privacy & Security** > **Stolen Device Protection** > Switch ON > Review **Require Security Delay** and choose the option best suited to your needs

  Strongly consider installing a reputable anti-virus app from the App Store. It can provide advanced theft alerts and monitor your device for potentially malicious activity.

7. Password protect app purchases

Control what's downloaded or purchased on your device through the App Store by requiring your password to be entered before a transaction can be completed:

- Navigate to **Settings** > **Screen Time** > **Content & Privacy Restrictions** > **iTunes & App Store Purchases** > Select **Always Require**

8. Phone Screening

This option makes unknown callers state why they are calling, and provides you with a transcript before your iPhone rings, allowing you to decide whether to answer the call.

- Navigate to **Settings** > **Apps** > **Phone**, scroll down, and under the **Screen Unknown Callers** section, select **Ask Reason for Calling**

9. Apple Intelligence & Siri

A personal intelligence system integrated into your iPhone, apps, and Siri.

- Navigate to **Settings** > **Apple Intelligence & Siri** > **Apple Intelligence** > Consider switching this feature OFF
- Scroll down to the **Extensions** section > Tap on an extension to review access settings
- Consider disabling **Setup Prompts** feature
- Review other features and adjust based on your level of comfort

SECURING YOUR SAMSUNG GALAXY — Operating System: Android 16

Limit your potential exposure

1. Lock your device

Enable a lock screen password to prevent unauthorized use of your device:

- Navigate to **Settings** > **Security and Privacy** > **Lock screen** > **Screen lock type** > Enter password (if prompted) > **Pin** > Enter a 6-digit passcode and confirm

Additionally, use Fingerprint or Facial Recognition to unlock your Samsung device with biometrics:

- Navigate to **Settings** > **Security and Privacy** > **Lock Screen** > **Screen Lock type** > **Fingerprints** > Follow activation steps

Tip: For added security, you can also set up Facial Recognition by selecting it under Screen lock type and following the activation instructions.

2. Limit information appearing on your lock screen

Android allows you to select the type of notification displayed on your locked Android device. “Hide content” will limit the information about the sender and message contents:

- Navigate to **Settings** > **Notifications** > **Lock screen notifications** > Switch ON: **Hide Content**

3. Disable tracking of your device

By default, Android tracks where you have taken your device. Disabling this feature will help protect you.

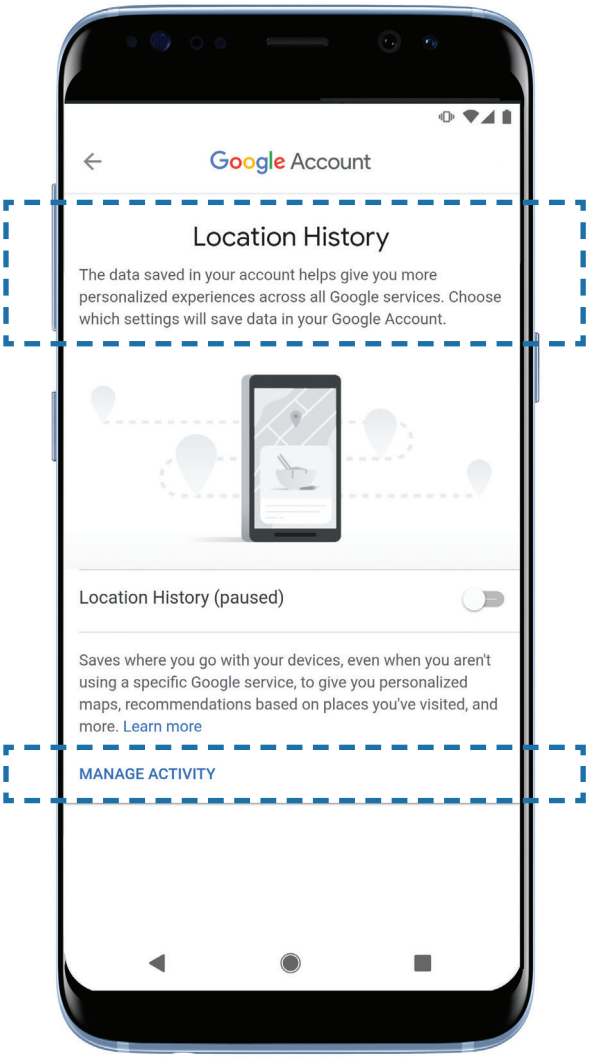
Disable Google Location History:

- Navigate to **Settings** > **Location** > **Location Services** > **Google Location History** > Choose **Google account** > Turn OFF: **Location History** > then select **Manage History** > **Menu** > **Settings and privacy** > **Delete all Location History**

4. Limit data tracking on your device

Your browser may save information about you and the websites you visit, such as usernames, passwords and addresses. To opt for security over convenience, disable this feature:

- Navigate to **Chrome** > **Menu** > **Settings** > **Payment Methods** > Switch OFF: **Save and fill payment methods**
- Navigate to **Chrome** > **Menu** > **Settings** > **Passwords** > Switch OFF: **Save passwords**



5. Find your device if it's misplaced, lost, or stolen

Android Device Manager allows you to locate the physical location of your device and also:

- Lock and reset device password
- Make device ring
- Remotely erase all data on your device

- Navigate to **Settings** > **Security and Privacy** > **Lost Device Protection** > Switch ON: **Find My Mobile** > **Follow activation steps**

Find My Device can be accessed via a web browser at: *https://findmymobile.samsung.com*

6. Password protect app purchases

Before making a purchase through the Google Play Store, ensure the transaction is password protected:

- Navigate to **Play Store** > **Tap the Profile icon** > **Settings** > **Authentication** > **Require authentication for purchases**

7. Manage the amount of personal information your apps can access

Many Google Play Store apps access your personal information. Consider not installing the ones that access your Device & App History, Device ID & Call Information Identity (profile data), Contacts, Wi-Fi Connections Information (including your Wi-Fi passwords), Bluetooth Connection Information and SMS Messages. To learn what information your apps can already access:

- Navigate to **Settings** > **Security and Privacy** > **Privacy** > **Permission manager**

As a general rule, be wary of free apps, as they are often a source of malware and/or viruses. It's best to download apps only from a trusted source.

Strongly consider installing a reputable mobile anti-virus app from the Google Play Store. It can help you monitor the information accessed and shared by your apps, as well as provide anti-virus protection.

8. Manage AI features

Samsung Galaxy devices running Android 16 may include AI-powered features such as smart assistants, photo enhancements, and personalized recommendations. To turn off certain AI features or use them securely:

To turn off AI features (such as Samsung's AI assistant or suggestions):

- Navigate to **Settings** > **Advanced Features** > **Samsung AI**
- Switch OFF: **AI features** (such as "Intelligent Suggestions," "Bixby," or other AI-powered options)

To use AI securely:

- Navigate to **Settings** > **Privacy** > **Permission manager**
  - Review and restrict permissions for apps using AI (such as camera, microphone, location, and contacts)
  - Regularly update your device to ensure the latest security patches for AI features
  - Be cautious about sharing sensitive information with AI-powered apps or assistants

Tip: Only enable AI features you trust and understand. Review privacy settings and permissions regularly to control what data is used by AI on your device.

SECURING YOUR ANDROID GOOGLE PIXEL — Operating System: Android 16

Limit your potential exposure

1. Lock your device

Enable a lock screen passcode to prevent unauthorized use of your device:

- Navigate to **Settings** > **Security and Privacy** > **Device Unlock** > **Screen lock** > Enter passcode (if prompted) > **PIN** > Enter a 6-digit passcode and confirm

Additionally, use Pixel Imprint if you prefer to unlock your Pixel with your fingerprint:

- Navigate to **Settings** > **Security & Privacy** > **Device Unlock** > Follow activation steps: **Fingerprint and Face Unlock**

2. Limit information appearing on your lock screen

Android allows you to select the type of notification displayed on your locked Android device. “Hide sensitive notification content” will limit the information about the sender and message contents:

- Navigate to **Settings** > **Security and Privacy** > **More Security and Privacy** > **Notifications on lock screen** > Switch OFF

3. Disable tracking of your device

By default, Android tracks where you have taken your device. Disabling this feature will help protect you.

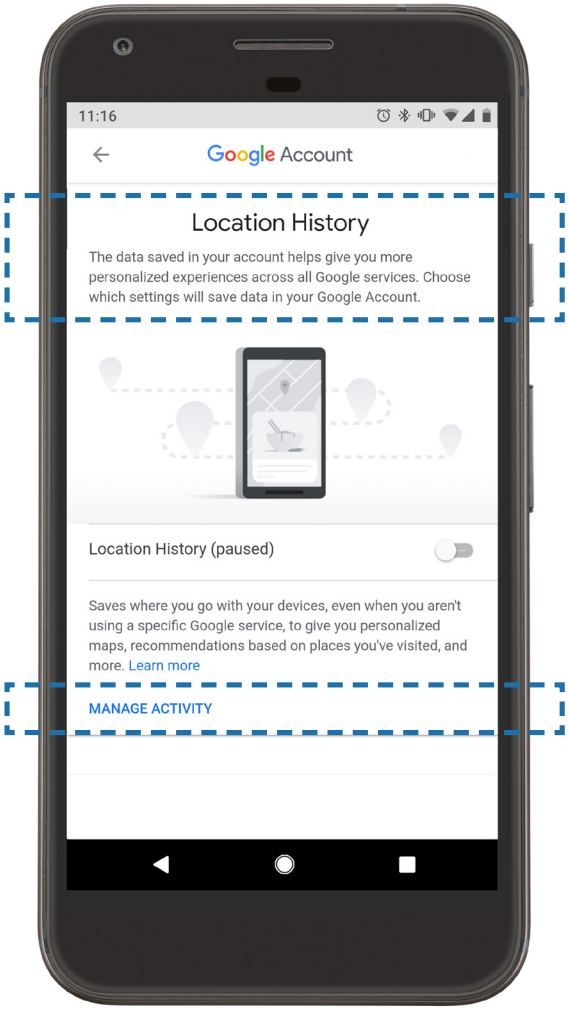
Disable Google Location History:

- Navigate to **Settings** > **Location** > **Location Services** > **Google Location History** > Switch OFF: **Location History** > then select **Manage Activity** > **Menu** > **Settings and privacy** > **Delete all Location History**

4. Limit data tracking on your device

Your browser may save information about you and the websites you visit, such as usernames, passwords and addresses. To opt for security over convenience, disable these features. For example:

- Navigate to **Chrome** > **Menu** > **Settings** > **Payment Methods** > **Save and fill payment methods** > Switch OFF
- Navigate to **Chrome** > **Menu** > **Settings** > **Google Password Manger** > **Settings** > **Offer to save passwords** > Switch OFF



5. Find your device if it's misplaced, lost, or stolen

Find My Device allows you to locate the physical location of your device and also:

- Lock and reset device password
- Make device ring
- Remotely erase all data on your device

- Navigate to **Settings** ⚙ > **Security and Privacy** > **Device Finders** > **Find Hub** > **Allow device to be located** > Switch ON

Find My Device can be accessed via a web browser at: *https://www.android.com/find*

6. Password protect app purchases

Before making a purchase through the Google Play Store, ensure the transaction is password protected:

- Navigate to **Play Store** > **Tap the Profile icon** > **Settings** > **Authentication** > **Require authentication for purchases**

7. Manage the amount of personal information your apps can access

Many Google Play Store apps access your personal information. Consider not installing the ones that access your Device & App History, Device ID & Call Information Identity (profile data), Contacts, Wi-Fi Connections Information (including your Wi-Fi passwords), Bluetooth Connection Information and SMS Messages. To learn what information your apps can already access:

- Navigate to **Settings** ⚙ > **Security and Privacy** > **Privacy Controls** > **Permission manager** > Regularly review and adjust privacy settings for all apps

As a general rule, be wary of free apps, as they are often a source of malware and/or viruses. It's best to download apps only from a trusted source.

Strongly consider installing a reputable mobile anti-virus app from the Google Play Store. It can help you monitor the information accessed and shared by your apps, as well as provide anti-virus protection.