CYBER SAFETY

Securing your Android Samsung S6 and S6 Edge*

Operating System: Android 6 Marshmallow

Your mobile device, which has made life so much more convenient, can track who you are, where you have been, and information about your friends, family and contacts. This can make you and your device a prime target for hackers. 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.

Limit your potential exposure

1. Lock your device

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

- Navigate to **Settings** ⚙ > **Lock screen and security** > **Screen lock type** > Enter password (if prompted) > **Password** > Enter your new secure password and confirm

Set your device to lock itself when it's not in use:

- Navigate to **Settings** ⚙ > **Lock screen and security** > **Secure lock settings** > **Lock automatically** > **Immediately** > Switch ON: **Lock instantly with power key**

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:

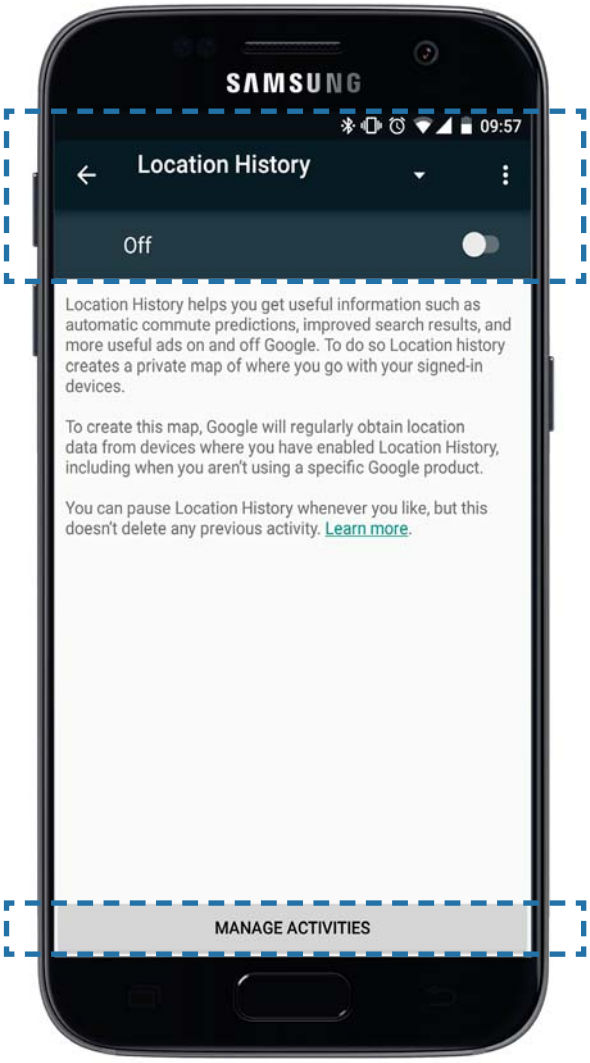
- Navigate to **Settings** ⚙ > **Lock screen and security** > **Notifications on lock screen** > **Hide Content**

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** > **Google Location History** > Switch OFF > Then select **Manage Activities** > **Menu** ⋮ > **Settings** > **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:

- For example, navigate to **Chrome** > **Menu** ⋮ > **Settings** > Switch OFF: **Autofill forms** and **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** ⚙ > **Google** > **Security** > Switch ON: **Remotely locate this device** and **Allow remote lock and erase**

Android Device Manager can be accessed via a web browser at: *https://www.google.com/android/devicemanager*

6. Password protect app purchases

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

- Navigate to **Play Store** > **Menu** ≡ > **Settings** ⚙ > **Require authentication for purchases** > **For all purchases through Google Play on this device**

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** ⚙ > **Applications** > **Application Manager** > Select an app > **Permissions**

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 *Lookout Security & Antivirus* 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.