J.P.Morgan

CYBER SAFETY

# Securing your credit*

In the United States, your identity and credit history can be used to secure loans and insurance policies, to gain employment, and to open credit cards. With so much at stake, it is essential to protect your credit, beginning with your credit report. Each of the U.S. credit bureaus provides tools to help minimize the risk of your credit report being used by unauthorized parties.

## monitor credit

Monitoring your credit report is the single best way to spot signs of identity theft, such as errors, suspicious activity and accounts or addresses you don't recognize. The three U.S. credit bureaus are required to provide one free credit report per year upon request. Any suspicious or fraudulent credit listing should be reported to the credit bureau that is showing the activity.

**THE THREE NATIONWIDE CREDIT BUREAUS HAVE SET UP A CENTRAL WEBSITE AND TELEPHONE NUMBER WHERE YOU CAN ORDER YOUR FREE ANNUAL REPORTS:**

877.322.8228 **www.annualcreditreport.com**

## implement a credit freeze

Also known as a **security freeze,** a credit freeze restricts access to your credit report, making it more difficult for identity thieves to open accounts in your name and/or abuse your credit. A credit freeze prevents a person, merchant or institution from making an inquiry about your credit report unless you temporarily lift or remove the freeze. Your credit report will continue to be accessible to your existing creditors or to debt collectors acting on their behalf.

Putting a credit freeze in place must be done separately with each of the three U.S. credit bureaus. Please note: The bureaus may charge for freeze requests; fees vary by state and according to local regulation. However, the cost of identity theft far outweighs any nominal fee incurred.

## lift a credit freeze

A credit freeze remains in place until you direct the credit bureau to either **temporarily lift** it or remove it entirely. For example, you can temporarily lift the credit freeze when you are applying for credit or employment. Similar to putting a credit freeze in place, each bureau charges a fee to unfreeze your credit, which varies by state. If possible, find out which credit bureau a merchant or prospective employer plans to use for its inquiry, and lift the freeze at that particular bureau. Please note: It can take up to three days for a bureau to lift a credit freeze.

**IN THE UNITED STATES, CONTACT EACH OF THE THREE CREDIT BUREAUS IF YOU WISH TO PUT A FREEZE IN PLACE OR LIFT A FREEZE:**

**Equifax**
800.349.9960
**freeze.equifax.com**

**Experian**
888.397.3742
**experian.com/freeze**

**TransUnion**
888.909.8872
**transunion.com/freeze**

## place a fraud alert

Placing a fraud alert on your credit file allows creditors to obtain a copy of your credit report—but they must take certain steps to verify your identity.

Fraud alerts may be effective at stopping someone from opening new credit accounts in your name; however, they may not prevent the misuse of your existing accounts. Fraud alerts do not freeze your credit, and they allow your credit score to change even as they mitigate the risk of unauthorized use. Please note: You only need to contact one credit bureau to have a fraud alert put in place, as that bureau is required to share the alert with the other two bureaus.

Three types of fraud alerts are available:

- **Initial Fraud Alert:** Principally designed for, but not reserved to, individuals who feel their identity has been compromised. Initial Fraud Alerts last 90 days from the date issued, are free of charge, and can be continuously renewed.
- **Extended Fraud Alert:** Reserved exclusively for victims of identity theft and designed to protect your credit for seven years.
- **Active Duty Military Alert:** Reserved for military personnel who want to protect their credit during deployment. Alerts last for one year and can be renewed.

### IN THE UNITED STATES, CONTACT ONE OF THE THREE CREDIT BUREAUS IF YOU WISH TO PLACE A FRAUD ALERT:

**Equifax**
888.766.0008
**equifax.com/CreditReportAssistance**

**Experian**
888.397.3742
**experian.com/fraudalert**

**TransUnion**
800.680.7289
**transunion.com/fraud**

 0115-0064-24 CSA-SECCRED-V3-112015

J.P.Morgan

CYBER SAFETY

# Securing your iOS device*

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.

## limit your potential exposure

### 1. Lock your device

Enable a passcode to prevent unauthorized use of your device:

**iOS 8**

- Go to **Settings** > **Touch ID & Passcode**; then scroll down to **Turn Passcode ON** and select *Passcode* **Options:** Select **Custom Numeric Code** and enter a passcode of at least 6 digits (which is 100 times more secure than a 4-digit passcode)

**iOS 9**

- Go to **Settings** > **Touch ID & Passcode**; then scroll down to **Turn Passcode ON** and enter a 6-digit passcode (iOS 9's enhanced security feature will prompt you for a 6-digit passcode)

Or, use **Touch ID Security** if you prefer to unlock your iOS device with your fingerprint: Go to **Settings** > **Touch ID & Passcode** > and scroll down to **Add a fingerprint**; then *switch ON:* **iPhone Unlock**

### 2. Limit information appearing on your lock screen

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

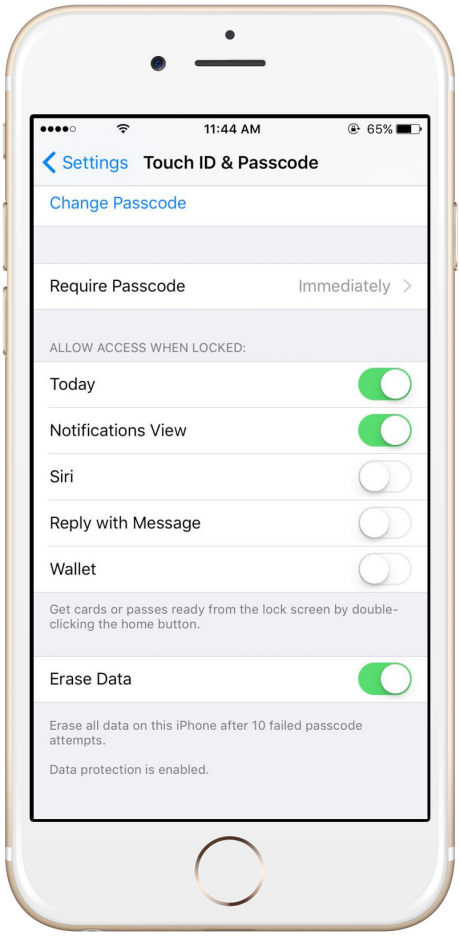
- Go to **Settings** > **Touch ID & Passcode** > **Enter Passcode** > **Allow Access When Locked**; then *switch OFF:* **Siri, Reply with Message** and **Wallet (Passbook in iOS 8)**

### 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:

- Go to **Settings** > **Touch ID & Passcode** > **Enter Passcode** > **Allow Access When Locked**; then *switch ON:* **Erase Data**

**Note:** Regularly back up your device to iCloud or your computer, via USB with iTunes, 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.

- Go to **Settings** > **Privacy** > **Location Services** > **System Services** > **Frequent Locations** > **Clear History** and *switch OFF*

## 5. Limit data and location tracking

### Maps and weather

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

- Go to **Settings** > **Privacy** > **Location Services** > **Individual Apps**; then change access for each one from Always to either **Never** or **While Using**

### Advertising

Limit advertisers from building a personal profile about you:

- Go to **Settings** > **Privacy** > **Advertising**; then *switch ON:* **Limit Ad Tracking** and select **Reset Advertising Identifier** and accept any prompts that follow

### Browser controls

Safari can save the personal information you use on websites, such as usernames, passwords and addresses. To opt for security over convenience, disable this feature:

- Go to **Settings** > **Safari** > **Passwords & Autofill**; then *switch OFF:* All options

## 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

- Go to **Settings** > **iCloud** > **Find My iPhone** (or iPad); then *switch ON*. Enter your device's passcode if prompted

## 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:

- Go to **Settings** > **iTunes & App Store** > **Password Settings**; then select **Always Require.** In addition, select **Require Password for Free Downloads**

J.P.Morgan

CYBER SAFETY

# Securing your Android HTC One M8/M9: Lollipop*

**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.**

## limit your potential exposure

### 1. Lock your device

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

- Go to **Settings** > **Security** > **Screen lock** > enter password (if prompted) > select **Password** > Create a new alphanumeric password using a combination of letters, numbers and special characters

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

- Go to **Settings** > **Security** > **Lock phone after** > **Immediately**

Stop "shoulder surfers" from viewing your password as you type:

- Go to **Settings** > **Security**; uncheck **Make passwords visible**

### 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:

- Go to **Settings** > **Sound and notification** > **When device is locked** and select **Hide sensitive notification content**

### 3. Disable tracking of your device

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

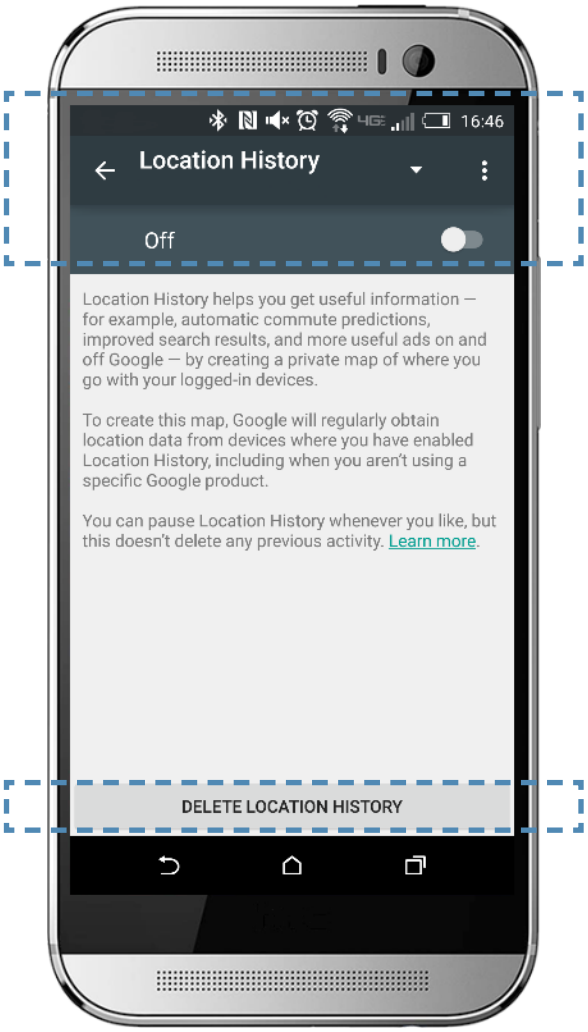
Disable Google Location History:

- Go to **Settings** > **Google Location History** > **Delete Location History** > and *switch OFF*

### 4. Limit data tracking on your device

Your browser can save information about you for websites you visit, such as usernames, passwords, and address. To secure sensitive information, disable this feature:

- For example, go 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

- Go to **Apps** > **Google Settings** > **Security** > *switch ON*: **Remotely locate this device** *and* **Allow remote lock and factory reset**

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:

- Go to **Play Store Settings** > **Require authentication for purchases** > select **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 can 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:

- Go to **Settings** > **Applications** > **Application Manager** > select an app > scroll down to **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 antivirus protection.

 0115-0064-19 CSA-HTCM9LOLLI-V5-112015

J.P.Morgan

CYBER SAFETY

# Securing your Android Samsung S6 Lollipop*

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.

## limit your potential exposure

### 1. Lock your device

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

- Go to **Settings** > **Lock screen and security** > **Screen lock type** > enter password (if prompted) > select **Password** > Create a new alphanumeric password using a combination of letters, numbers and special characters

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

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

Stop "shoulder surfers" from viewing your password as you type:

- Go to **Settings** > **Lock screen and security** > **Other security settings** > *switch OFF:* **Make passwords visible**

### 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:

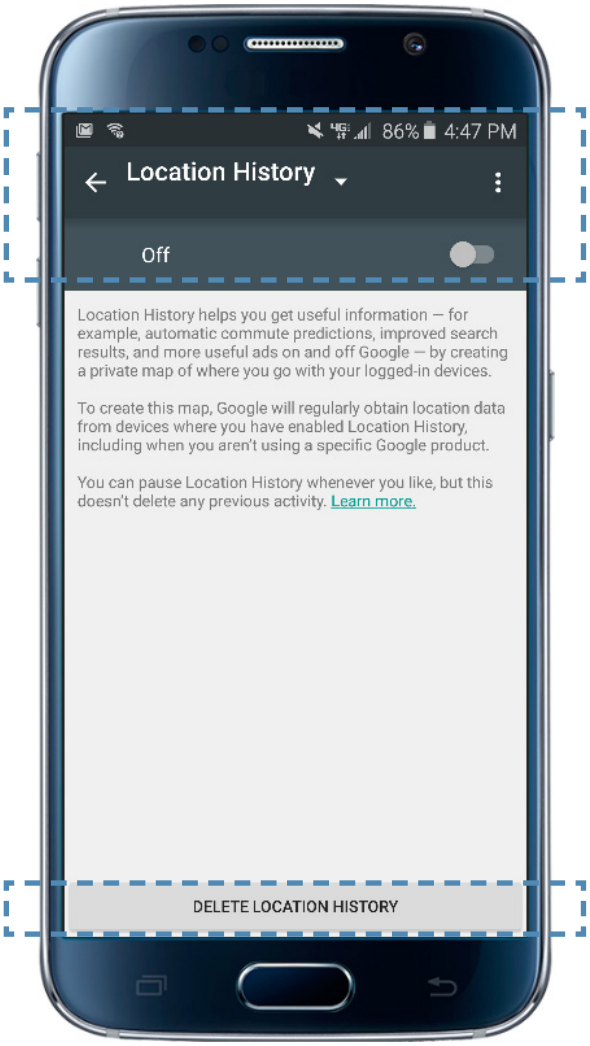
- Go to **Settings** > **Sound and notification** > **Notifications on lock screen** > and select **Hide Content**

### 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:

- Go to **Settings** > **Google Location History** > **Delete Location History** > and *switch OFF*



## 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, go 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

- Go to **Apps** > **Google** > **Google Settings** > **Security** > *switch ON:* **Remotely locate this device** *and* **Allow remote lock and factory reset**

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:

- Go to **Play Store Settings** > **Require authentication for purchases** > select **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:

- Go to **Settings** > **Applications** > **Application Manager** > select an app > scroll down to **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 antivirus protection.

 0115-0064-13

CSA-SAMS6LOLLI-V5-112015