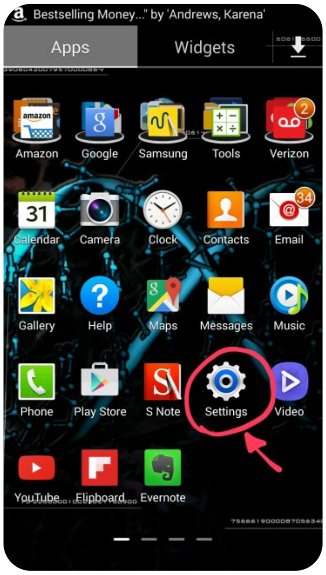
Guide to Securing Android Devices

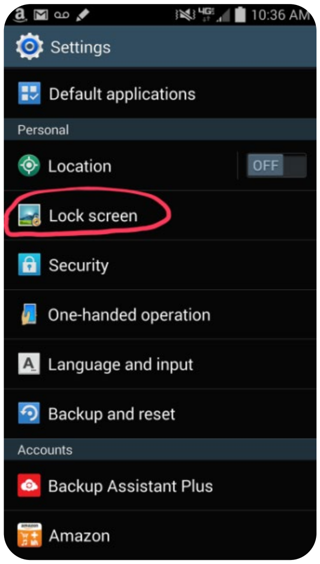
Purpose: This guide is meant to assist in applying the minimum security settings required on android devices. Due to the broad scope of android devices, this is only meant as a general guide and actual procedures may vary between different devices.

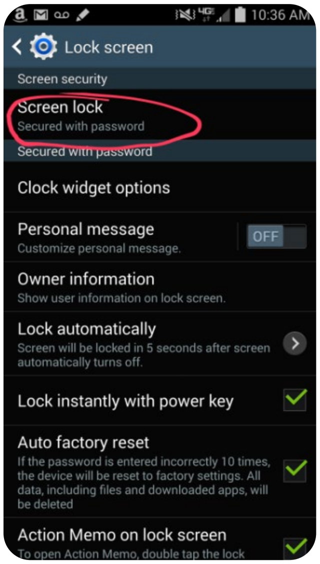
Most of the needed security settings can be found by **clicking on the "Settings" icon** in the applications menu.



Require a password, PIN, or passcode for access. This prevents others from using your device by requiring the passcode to unlock it.

Under settings **click on "Lock Screen"** then **click on "Screen lock"** and set a password that is complex but easy to remember.





10:36 AM

Lock screen

Screen security

Screen lock
Secured with password

Secured with password

Clock widget options

Personal message
Customize personal message. OFF

Owner information
Show user information on lock screen.

Lock automatically
Screen will be locked in 5 seconds after screen automatically turns off.

Lock instantly with power key ✓

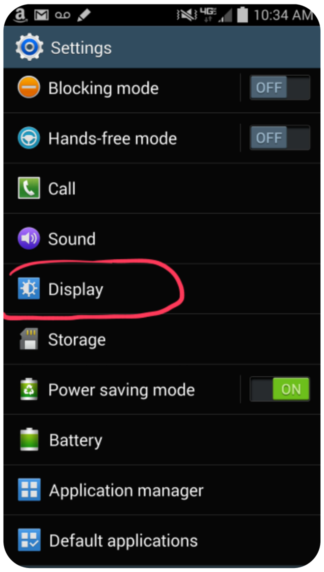
Auto factory reset
If the password is entered incorrectly 10 times, the device will be reset to factory settings. All data, including files and downloaded apps, will be deleted ✓

Action Memo on lock screen
To open Action Memo, double tap the lock ✓

For assistance and additional information, please visit the GRCC IT Security webpage at http://grcc.edu/informationtechnology/itsecurity or contact the Help Desk at ITHELP@GRCC.EDU

Set the screen lock to auto lock after 15 or fewer minutes of inactivity. This, in conjunction with your password/PIN/passcode, protects your device from unauthorized use and helps conserve battery power.

From the settings screen **click on "Display"** and then **click on "Screen timeout"**. Set a time limit of less than 15 minutes.



10:34 AM

Settings

Blocking mode OFF

Hands-free mode OFF

Call

Sound

Display

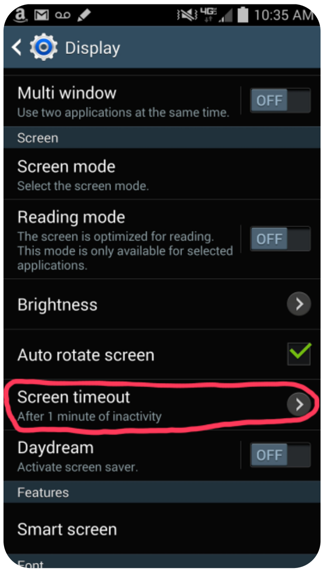
Storage

Power saving mode ON

Battery

Application manager

Default applications



10:35 AM

Display

Multi window OFF
Use two applications at the same time.

Screen

Screen mode
Select the screen mode.

Reading mode OFF
The screen is optimized for reading. This mode is only available for selected applications.

Brightness

Auto rotate screen ✓

Screen timeout
After 1 minute of inactivity

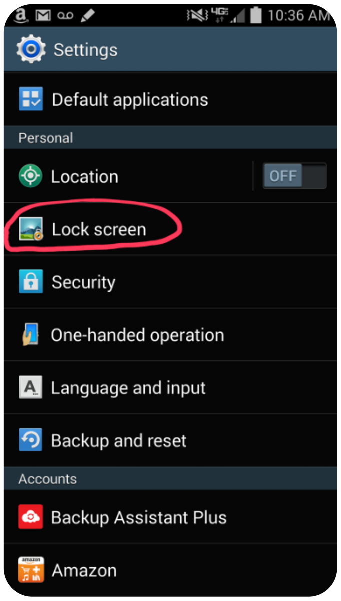
Daydream OFF
Activate screen saver.

Features

Smart screen

Font

In the Lock screen menu **click on "Lock automatically"** and set a time limit so the total combined time of screen timeout and lock screen time is less than 15 minutes.



10:36 AM

Settings

Default applications

Personal

Location OFF

Lock screen

Security

One-handed operation

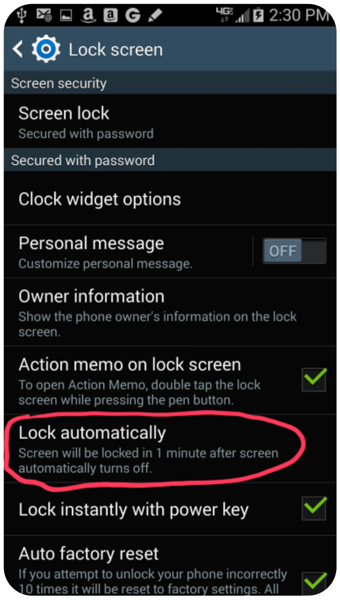
Language and input

Backup and reset

Accounts

Backup Assistant Plus

Amazon



2:30 PM

Lock screen

Screen security

Screen lock
Secured with password

Secured with password

Clock widget options

Personal message OFF
Customize personal message.

Owner information
Show the phone owner's information on the lock screen.

Action memo on lock screen ✓
To open Action Memo, double tap the lock screen while pressing the pen button.

Lock automatically
Screen will be locked in 1 minute after screen automatically turns off.

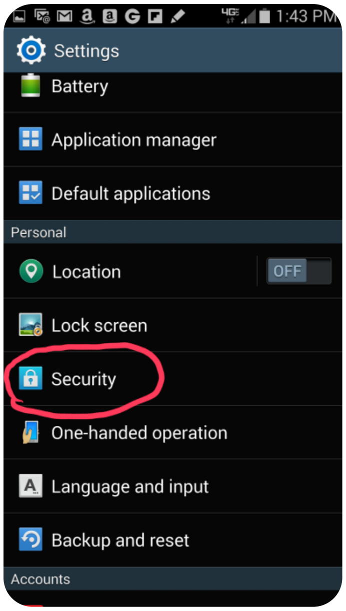
Lock instantly with power key ✓

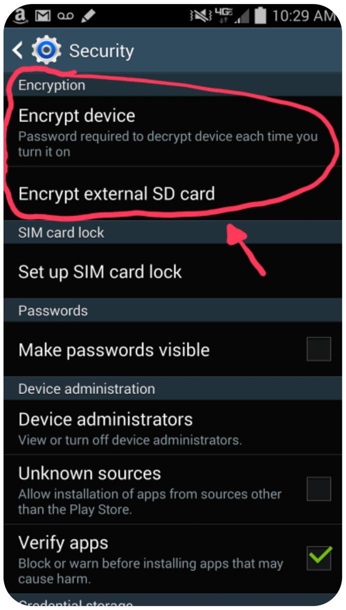
Auto factory reset ✓
If you attempt to unlock your phone incorrectly 10 times it will be reset to factory settings. All

For assistance and additional information, please visit the GRCC IT Security webpage at http://grcc.edu/informationtechnology/itsecurity or contact the Help Desk at ITHELP@GRCC.EDU

Turn on data encryption. This prevents others from accessing the data on your device.

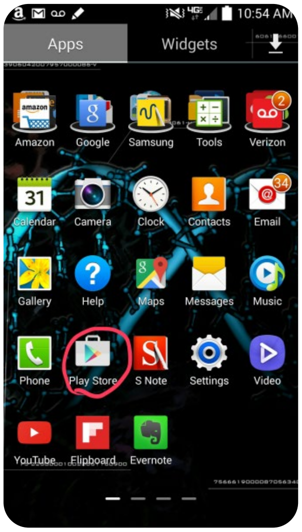
From the settings screen, **Click on "Security**" then **click on "Encrypt device"** and **"Encrypt external SD card"**.

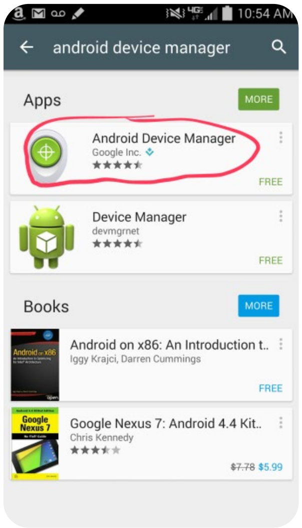


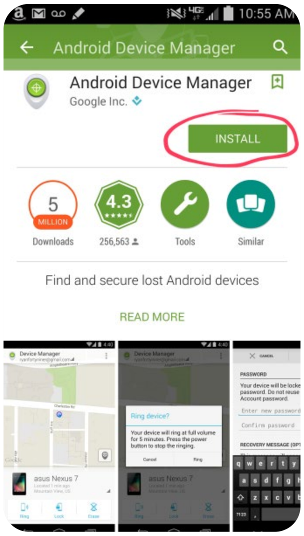

10:29 AM
Security
Encryption
Encrypt device
Password required to decrypt device each time you turn it on
Encrypt external SD card
SIM card lock
Set up SIM card lock
Passwords
Make passwords visible
Device administration
Device administrators
View or turn off device administrators.
Unknown sources
Allow installation of apps from sources other than the Play Store.
Verify apps
Block or warn before installing apps that may cause harm.
Credential storage

Install and use a device tracking app. Such an app will help you track or remotely erase your device if it is lost or stolen.

A free app that can be used for remote tracking and data wiping is the Android Device Manager. To install this, from the applications menu, **click on the "Play Store" app**. Use the magnifying glass in the upper right corner to **type in and search for the Android Device Manager. Click on it** and then **click "INSTALL"**. Once installed, open the app and follow the onscreen instructions.



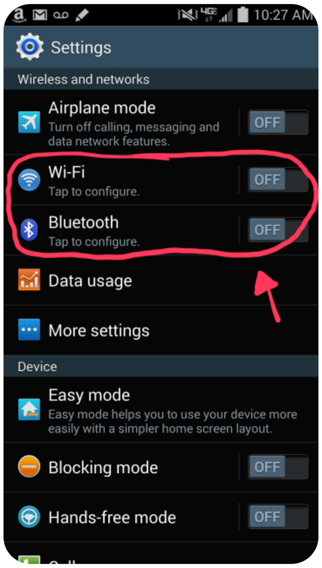




For assistance and additional information, please visit the GRCC IT Security webpage at http://grcc.edu/informationtechnology/itsecurity or contact the Help Desk at ITHELP@GRCC.EDU

When not using Wi-Fi and Bluetooth, turn them off. This prevents unauthorized access to your device through those connections.

You can turn off Wi-Fi and Bluetooth from the Settings screen as shown below.



10:27 AM

Settings

Wireless and networks

Airplane mode
Turn off calling, messaging and data network features. OFF

Wi-Fi
Tap to configure. OFF

Bluetooth
Tap to configure. OFF

Data usage

More settings

Device

Easy mode
Easy mode helps you to use your device more easily with a simpler home screen layout.

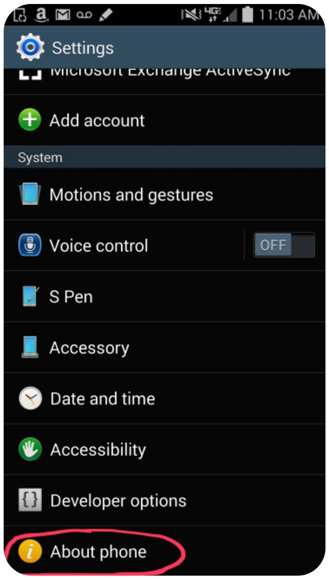
Blocking mode OFF

Hands-free mode OFF

Keep your Android firmware and apps updated. This helps ensure you have the latest security updates installed.

Your phone should prompt you automatically when updates for applications are available. Click on the prompt and accept the update.

For updating the phones firmware and software, **click on "About phone"** from the Settings screen. Then click on "Software update".



11:03 AM

Settings

Microsoft Exchange ActiveSync

Add account

System

Motions and gestures

Voice control OFF

S Pen

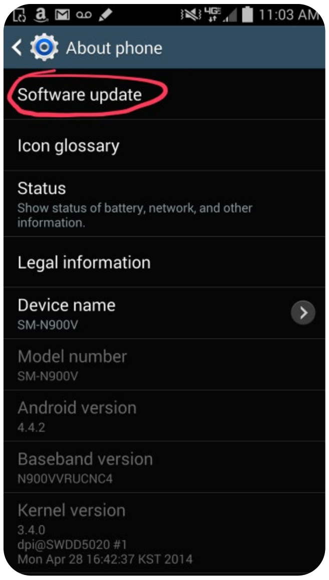
Accessory

Date and time

Accessibility

Developer options

About phone



11:03 AM

About phone

Software update

Icon glossary

Status
Show status of battery, network, and other information.

Legal information

Device name
SM-N900V

Model number
SM-N900V

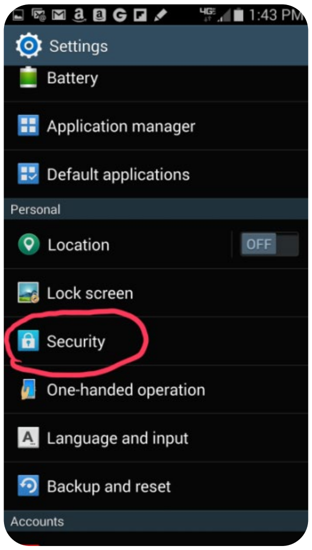
Android version
4.4.2

Baseband version
N900VVRUCNC4

Kernel version
3.4.0
dpi@SWDD5020 #1
Mon Apr 28 16:42:37 KST 2014

Only install trusted market apps, such as Google Play or Amazon Marketplace apps. This helps avoid installing malware that may be hiding in untrusted apps.

From the settings screen **click on "Security"** then **ensure "Unknown sources" is unchecked** and **"Verify apps" is checked** as shown below.



1:43 PM

Settings

Battery

Application manager

Default applications

Personal

Location OFF

Lock screen

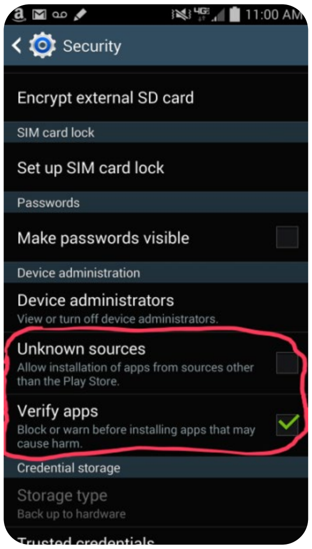
Security

One-handed operation

Language and input

Backup and reset

Accounts



11:00 AM

Security

Encrypt external SD card

SIM card lock

Set up SIM card lock

Passwords

Make passwords visible □

Device administration

Device administrators
View or turn off device administrators.

Unknown sources □
Allow installation of apps from sources other than the Play Store.

Verify apps ☑
Block or warn before installing apps that may cause harm.

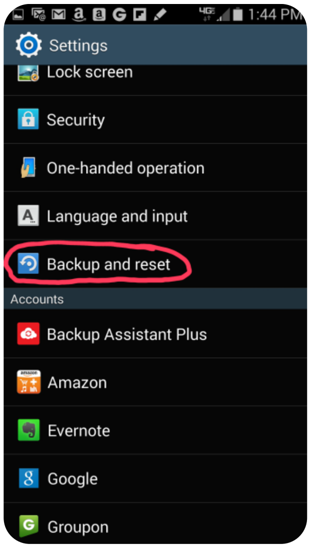
Credential storage

Storage type
Back up to hardware

Trusted credentials

Before you sell or give away your device, erase all content and settings. This prevents others from accessing your data.

Click on "Backup and reset" from the Settings screen. Please note that the Factory data reset will delete all the data on the phone and you will lose any information you have not backed up to a secure location.



1:44 PM

Settings

Lock screen

Security

One-handed operation

Language and input

Backup and reset

Accounts

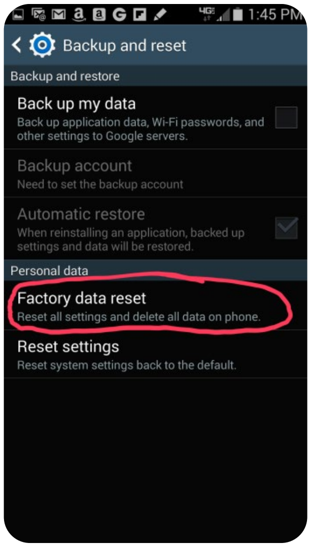
Backup Assistant Plus

Amazon

Evernote

Google

Groupon



1:45 PM

Backup and reset

Backup and restore

Back up my data □
Back up application data, Wi-Fi passwords, and other settings to Google servers.

Backup account
Need to set the backup account

Automatic restore ☑
When reinstalling an application, backed up settings and data will be restored.

Personal data

Factory data reset
Reset all settings and delete all data on phone.

Reset settings
Reset system settings back to the default.

For assistance and additional information, please visit the GRCC IT Security webpage at http://grcc.edu/informationtechnology/itsecurity or contact the Help Desk at ITHELP@GRCC.EDU