Independent Skill Development Mission

Independent Skill Development Mission NXT
EMPOWERING FUTURES, SHAPING TOMORROW

ISDM (INDEPENDENT SKILL DEVELOPMENT MISSION

INTRODUCTION TO MOBILE UNLOCKING (NETWORK UNLOCK & BOOTLOADER UNLOCK)

UNDERSTANDING MOBILE UNLOCKING

Mobile unlocking refers to the **process of removing restrictions imposed by manufacturers or network carriers**, allowing users to switch carriers, install custom firmware, or modify system files.

There are **two primary types of mobile unlocking**:

1. **Network Unlocking** – Unlocks a phone from a specific carrier, allowing it to be used with any network provider.
2. **Bootloader Unlocking** – Unlocks the device bootloader, enabling the installation of **custom ROMs, kernels, and root access**.

Unlocking provides **greater flexibility, enhanced customization, and extended device lifespan**, but it also comes with risks such as **warranty voidance, security vulnerabilities, and potential bricking of the device**.

NETWORK UNLOCKING – REMOVING CARRIER RESTRICTIONS

What is Network Unlocking?

Network unlocking allows a mobile phone **to use SIM cards from different network carriers**. Many devices are locked to a specific carrier by default, preventing users from switching networks.

Why Do Manufacturers Lock Phones to a Network?

✓ **To ensure customer loyalty** – Carriers want users to stay on their network.
✓ **To recover device subsidies** – Many phones are sold at a discount, with the cost recovered over a contract period.
✓ **To prevent unauthorized resale** – Locked phones cannot be used on other networks unless unlocked.

Methods of Network Unlocking

1. **Unlock Code from Carrier:**
   - Users can request an unlock code from the original network provider.
   - The code is entered in the phone's **Network Unlock Screen** to remove restrictions.
2. **Third-Party Unlocking Services:**
   - Online services provide network unlock codes based on IMEI.
   - These services charge a fee and are useful if the carrier refuses to unlock the device.
3. **Software-Based Unlocking:**
   - Some older phones can be unlocked using special software tools.
   - This method is rare in modern smartphones due to enhanced security.

4. **Unlocking via Root Access (For Advanced Users):**
   - Some Android devices allow network unlocking by modifying system files.
   - Requires **root access** and risks **permanent damage or bricking**.

Steps to Unlock a Network-Locked Phone via Carrier

1. **Find the IMEI Number**: Dial *#06# to get the IMEI.
2. **Contact the Carrier**: Request an unlock code if eligible.
3. **Enter the Unlock Code**: Insert a new SIM card and enter the provided code.
4. **Restart and Test**: The device should now accept any SIM card.

✓ **Outcome:** The phone can now use SIM cards from multiple network providers.

Example: Unlocking a Network-Locked Samsung Galaxy S22

A user buys a **Samsung Galaxy S22** from **AT&T**, but wants to switch to **T-Mobile**. Since the contract is complete, they request an unlock code from AT&T. After entering the code, the phone becomes **carrier-unlocked**, allowing it to work with any SIM card.

Bootloader Unlocking – Gaining Full Control Over the Device

What is Bootloader Unlocking?

The **bootloader** is the first program that runs when a phone is powered on. It initializes hardware and loads the operating system. By default, bootloaders are **locked** to prevent unauthorized modifications.

Unlocking the bootloader allows **custom ROM installation, rooting, and deep system modifications**.

Why is the Bootloader Locked?

✓ **To ensure device security** – Prevents malware and unauthorized system changes.

✓ **To restrict software modifications** – Manufacturers want users to stick to official updates.

✓ **To prevent warranty claims on modified devices** – Bootloader unlocking often voids the warranty.

Advantages of Unlocking the Bootloader

✓ Allows installation of **Custom ROMs** (LineageOS, Pixel Experience, etc.).

✓ Enables **root access** for advanced customizations.

✓ Provides access to **custom kernels** for better performance and battery life.

✓ Supports **advanced debugging and system modifications**.

Disadvantages of Unlocking the Bootloader

✕ **Voids warranty** on most devices.

✕ **Increases the risk of bricking** if done incorrectly.

✕ **May cause security vulnerabilities**, making the phone susceptible to malware.

HOW TO UNLOCK THE BOOTLOADER (STEP-BY-STEP GUIDE)

1. Check if the Bootloader is Unlockable

- Some devices allow unlocking, while others (e.g., some Samsung and Huawei phones) do not.
- To check, open the dialer and enter:
- fastboot oem device-info

If it says "Unlocked: No," then it can be unlocked.

2. Enable Developer Options & OEM Unlocking

1. Go to **Settings** → **About Phone** → **Tap 'Build Number' 7 times**.
2. Navigate to **Developer Options** → **Enable OEM Unlocking**.

3. Boot the Phone into Fastboot Mode

1. Power off the device.
2. Press and hold **Power + Volume Down** to enter **Fastboot Mode**.

4. Connect the Device to a PC & Use Fastboot Commands

1. Install **ADB & Fastboot tools** on your computer.
2. Open a command prompt and type:
3. fastboot oem unlock
4. Confirm the unlocking process on the phone.

5. Reboot the Device

- Type the following command:

- fastboot reboot
- The phone will now boot with an **unlocked bootloader**.

✓ **Outcome:** The device is ready for custom ROM installation and advanced modifications.

Example: Unlocking the Bootloader on a Xiaomi Phone

A user wants to install **Pixel Experience ROM** on their **Redmi Note 10**. Since Xiaomi requires **Mi Unlock Tool**, the user:

1. Requests **Bootloader Unlock Permission** from Xiaomi.
2. Uses **Mi Unlock Tool** to unlock the bootloader.
3. Installs a **custom recovery (TWRP)** and then flashes Pixel Experience.

✓ **Result:** The Xiaomi phone runs a **custom, bloatware-free ROM**.

Comparison of Network Unlock & Bootloader Unlock

Feature	**Network Unlock**	**Bootloader Unlock**
Purpose	Allows the phone to work with different carriers	Enables system modifications & custom ROMs
Risk Level	Low (if done via carrier)	High (can brick device)
Warranty Status	Usually unaffected	Often voids warranty

Tools Required	Unlock code, carrier request	ADB, Fastboot, Unlock tool

Case Study: Unlocking a Carrier-Locked & Bootloader-Locked Phone

Scenario:

A user buys a **OnePlus 8T** from **T-Mobile** but wants to:

1. **Use it with another carrier (Network Unlock).**
2. **Install a custom ROM (Bootloader Unlock).**

Solution:

✓ **Step 1:** The user **requests an unlock code from T-Mobile** and enters it, allowing SIM card compatibility with all networks.
✓ **Step 2:** The user **enables OEM Unlocking** and unlocks the bootloader using Fastboot.
✓ **Step 3:** The user installs **LineageOS** for a **custom Android experience**.

✓ **Result:** The OnePlus 8T is **fully unlocked** for both network and bootloader modifications.

Exercise

1. **What is the difference between network unlocking and bootloader unlocking?**
2. **List two advantages and two risks of unlocking the bootloader.**

3. **Describe the step-by-step process of unlocking the bootloader on an Android phone.**
4. **Why do manufacturers lock bootloaders and network carriers?**
5. **What tools are used for bootloader unlocking?**

CONCLUSION

✓ Network unlocking allows SIM flexibility, while bootloader unlocking enables deep system modifications.
✓ Bootloader unlocking is required for installing custom ROMs and rooting devices.
✓ While unlocking offers benefits, it also introduces risks like voided warranties and security vulnerabilities.
✓ Understanding these unlocking methods helps mobile technicians modify and repair devices effectively.

UNDERSTANDING IMEI REPAIR TECHNIQUES

INTRODUCTION TO IMEI AND ITS IMPORTANCE

The **IMEI (International Mobile Equipment Identity)** is a **15-digit unique identifier** assigned to every mobile phone. It plays a **crucial role in identifying devices on mobile networks** and helps in **tracking lost or stolen phones, network authentication, and device security**.

However, in certain cases, the IMEI number may get **corrupted, lost, or changed** due to:
✓ Flashing stock/custom firmware incorrectly.
✓ Formatting NVRAM on MediaTek devices.
✓ Network unlocking issues.
✓ Physical motherboard damage.
✓ Software errors or malicious activities.

When an IMEI is lost or invalid, the device **cannot register on the network**, leading to **"No Service" or "Invalid IMEI" errors**. This guide explores **various IMEI repair techniques** to restore lost or corrupted IMEIs and make the device functional again.

UNDERSTANDING THE CAUSES OF IMEI LOSS OR CORRUPTION

What Causes IMEI to Get Lost or Corrupted?

1. **Flashing Incorrect Firmware**
   - Some firmware updates do not contain correct IMEI information, leading to a lost IMEI.

2. **Corrupted or Wiped NVRAM (Non-Volatile RAM)**
   - NVRAM stores **network-related settings, including IMEI information**.
   - Formatting NVRAM using SP Flash Tool can erase the IMEI.
3. **Using Unofficial Unlocking Methods**
   - Some third-party unlocking tools **alter the IMEI** and corrupt network connectivity.
4. **Factory Reset or Hard Reset Issues**
   - In some cases, resetting the phone can cause **IMEI mismatches or loss**.
5. **Malware or Viruses**
   - Some malicious software **modifies IMEI numbers**, leading to network restrictions.

How to Check If IMEI is Lost or Corrupted?

✓ **Dial *#06# to view the IMEI number.**
✓ If the device shows **"Invalid IMEI" or "Null IMEI"**, it means the IMEI is lost.
✓ **Check NVRAM status:** In some MediaTek phones, enter *#4634# to verify if NVRAM is intact.

Techniques for IMEI Repair

1. Restoring IMEI Using Engineer Mode (For MediaTek Devices)

MediaTek (MTK) phones allow IMEI repair via the **Engineering Mode menu**, which can be accessed through a secret code.

Steps to Repair IMEI via Engineer Mode:

1. **Dial *#*#3646633#*#* to enter Engineering Mode.**
2. Navigate to **Connectivity** → **CDS Information** → **Radio Information.**
3. Select **Phone 1** (for SIM 1) and enter the IMEI command:
4. AT+EGMR=1,7,"IMEI_NUMBER"
5. Select **Phone 2** (for SIM 2) and enter the IMEI command:
6. AT+EGMR=1,10,"IMEI_NUMBER"
7. Click **Send AT Command** and reboot the phone.

✓ **Outcome:** The phone restores the lost IMEI and reconnects to the mobile network.

---

2. Using Maui Meta Tool (For Advanced MediaTek IMEI Repair)

Maui Meta Tool is a professional tool used to repair IMEI on **MediaTek devices** by modifying the **NVRAM database file (NVRAM.bin)**.

Steps to Repair IMEI Using Maui Meta Tool:

1. **Download and Install Maui Meta Tool on PC.**
2. **Power off the phone and connect it in Meta Mode** (Hold Volume Down while connecting USB).
3. **Select 'IMEI Download' and Load the Database File (NVRAM.bin).**

4. **Enter the Original IMEI and Click 'Write'.**
5. **Reboot the Device and Check IMEI with *#06#.**

✓ **Outcome:** The IMEI is restored, allowing the phone to reconnect to the mobile network.

---

3. Using SN Write Tool for IMEI Restoration (For MediaTek Devices)

SN Write Tool is an alternative to **Maui Meta Tool** and is used to **restore IMEI, Wi-Fi MAC, Bluetooth Address, and Serial Numbers**.

Steps to Repair IMEI Using SN Write Tool:

1. **Install SN Write Tool and MediaTek USB Drivers.**
2. **Open SN Write Tool and Select 'IMEI Download'.**
3. **Load the 'AP_DB' and 'MD_DB' files from stock firmware.**
4. **Enter the original IMEI numbers.**
5. **Click 'Start' and connect the device in Meta Mode.**
6. **Once writing is successful, restart the phone.**

✓ **Outcome:** The lost IMEI is restored, and network registration works properly.

---

4. Using QCN Rebuilder for Qualcomm Devices

For **Qualcomm (Snapdragon) phones**, IMEI can be restored using **QCN (Qualcomm Calibration Network) files**.

Steps to Restore IMEI Using QCN Rebuilder:

1. **Install QPST Tool and Connect the Phone in Diagnostic Mode.**
2. **Backup the Existing QCN File Using QPST.**
3. **Edit the QCN File Using QCN Rebuilder and Add the Correct IMEI.**
4. **Restore the Modified QCN File Back to the Device.**
5. **Reboot and Check the IMEI Status (*#06#).**

✓ **Outcome:** The Qualcomm device restores network connectivity.

CASE STUDY: IMEI LOSS DUE TO FIRMWARE FLASHING

Scenario:

A technician receives a **Realme C15 (MediaTek Helio G35)** that shows **"Invalid IMEI"** after flashing stock firmware. The device **cannot register on the network**, and calling *#06# shows a **null IMEI**.

Solution:

✓ **Step 1:** Checked the IMEI status using ***#06#** and confirmed it was missing.
✓ **Step 2:** Used **Maui Meta Tool** to rewrite the original IMEI using **NVRAM.bin**.
✓ **Step 3:** Rebooted the phone and verified the IMEI was restored.

✓ **Result:** The phone successfully reconnected to the mobile network, resolving the IMEI issue.

Comparison of IMEI Repair Methods

Method	**Supported Chipsets**	**Difficulty Level**	**Risk Level**
Engineer Mode	MediaTek (MTK)	Easy	Low
Maui Meta Tool	MediaTek (MTK)	Medium	Moderate
SN Write Tool	MediaTek (MTK)	Medium	Low
QCN Rebuilder	Qualcomm (Snapdragon)	Hard	High

Exercise

1. **What is the IMEI number, and why is it important?**
2. **List three reasons why IMEI might be lost or corrupted.**
3. **Explain how the Maui Meta Tool helps in IMEI restoration.**
4. **Which IMEI repair tool is used for Qualcomm devices?**
5. **Describe the risks associated with IMEI repair and modification.**

Conclusion

✓ IMEI is essential for network connectivity, device identification, and security.
✓ IMEI loss is common after firmware flashing, NVRAM

corruption, and unauthorized unlocking.

✓ Engineer Mode and Maui Meta Tool are effective for repairing IMEI on MediaTek devices.

✓ QCN Rebuilder helps restore IMEI on Qualcomm-based phones.

✓ Technicians must ensure that they are restoring the original IMEI legally and ethically.

BYPASSING GOOGLE FRP LOCK (FACTORY RESET PROTECTION)

UNDERSTANDING GOOGLE FRP LOCK

What is FRP (Factory Reset Protection)?

Factory Reset Protection (FRP) is a **security feature developed by Google** to protect Android devices from **unauthorized access after a factory reset**. When a user resets their device, FRP **prevents access to the phone unless the original Google account credentials are entered**.

Why Does FRP Exist?

✓ Prevents unauthorized use of stolen/lost devices.
✓ Ensures only the legitimate owner can reset and access the phone.
✓ Increases Android device security, especially after a hard reset.

When Does FRP Activate?

FRP is automatically enabled when:
✓ A **Google account is added** to an Android device.
✓ The device undergoes a **factory reset without removing the Google account first**.

FRP Lock Message:

After a reset, users see:
"This device was reset. To continue, sign in with a Google account previously synced on this device."

If the owner forgets their Google credentials or buys a second-hand locked phone, FRP must be bypassed to regain access.

Methods to Bypass Google FRP Lock

1. Using the “Forgot Email” Option (If You Own the Device)

If you **forgot your Google account credentials** but still have access to **your registered email or phone number**, follow these steps:

Steps to Recover Google Account:

1. On the FRP screen, select **"Need help finding your account?"**
2. Enter a **phone number or recovery email** linked to the Google account.
3. Follow the **password reset instructions** sent to your email.
4. After resetting the password, enter the new credentials on the locked device.

✓ **Outcome:** The phone unlocks successfully using the recovered Google account.

2. Bypassing FRP via Emergency Call Trick (For Older Android Versions)

On some older Android versions (Android 7 and below), the **Emergency Call feature** can be used to bypass FRP.

Steps to Bypass FRP via Emergency Call:

1. **On the Google verification screen, tap "Emergency Call."**
2. Dial *#*#4636#*#* to open the **Testing Menu** (works on some devices).
3. Tap **Usage Statistics** → **Back button** to enter **Settings**.

4. Enable **Developer Options** → **OEM Unlocking** and restart the phone.

✓ **Outcome:** The device boots up without the FRP lock.

---

3. Using FRP Bypass APK (For Android 8 & 9 Devices)

Android devices running **Android 8, 9, and some Android 10 versions** can be bypassed using **FRP Bypass APK files**.

Steps to Bypass FRP Using APK Installation:

1. **Connect the device to Wi-Fi** and return to the **Google Account Verification page**.
2. On the keyboard, tap and hold the @ symbol, then **go to Google Keyboard Settings**.
3. Select **Help & Feedback** → **Search "Use Morse Code"** and **Play YouTube Video**.
4. Tap **Share** on the video → Open Chrome browser.
5. Download **FRP Bypass APK** from a trusted website.
6. Install and open the APK → Tap **"Bypass FRP"** → Select **"Sign in with a new account"**.
7. Enter a **new Google account** and restart the device.

✓ **Outcome:** The device successfully bypasses FRP with a new Google account.

---

4. Bypassing FRP Using Samsung FRP Tool (For Samsung Devices)

Samsung phones have additional security layers, making FRP removal difficult. **Samsung FRP Tool** is a dedicated solution for **bypassing Google FRP on Samsung devices**.

Steps to Bypass FRP Using Samsung FRP Tool:

1. Download and install **Samsung FRP Tool** on a PC.
2. **Boot the phone into Download Mode (Power + Volume Down + Bixby).**
3. Connect the phone to the PC via USB.
4. Open **Samsung FRP Tool** and click **"Remove FRP"**.
5. The phone reboots automatically.
6. On the setup screen, enter **a new Google account**.

✓ **Outcome:** FRP is successfully removed from the Samsung phone.

Advanced FRP Bypass Techniques (For Technicians)

1. Using ADB Commands (For Advanced Users)

Android Debug Bridge (**ADB**) commands can remove FRP if **USB Debugging is enabled**.

Steps to Bypass FRP Using ADB Commands:

1. **Connect the phone to a PC using a USB cable.**
2. Open **Command Prompt** on the PC.
3. Type the following commands one by one:
4. adb shell

5. rm -rf /data/system/gesture.key
6. rm -rf /data/system/accounts.db
7. reboot
8. The phone reboots, and FRP is removed.

✓ **Outcome:** The phone boots without the FRP lock.

Case Study: Unlocking a Google-Locked Samsung Galaxy A51

Scenario:

A technician receives a **Samsung Galaxy A51** with **Google FRP lock** after a factory reset. The customer **forgot their Google account credentials** and cannot access the phone.

Solution:

✓ **Step 1:** The technician downloads **Samsung FRP Tool** on a PC.
✓ **Step 2:** The phone is booted into **Download Mode (Power + Volume Down + Bixby).**
✓ **Step 3:** The device is connected via USB, and **FRP is removed using Samsung FRP Tool.**
✓ **Step 4:** The phone restarts, and a **new Google account is added.**

✓ **Result:** The Samsung Galaxy A51 is **fully unlocked and ready for use.**

Comparison of FRP Bypass Methods

Method	**Best for**	**Difficulty Level**	**Success Rate**
Forgot Email Option	Users who own the account	Easy	High
Emergency Call Trick	Older Android versions	Medium	Moderate
FRP Bypass APK	Android 8 & 9	Hard	High
Samsung FRP Tool	Samsung phones	Medium	High
ADB Commands	Advanced users	Very Hard	Moderate

Exercise

1. **What is Factory Reset Protection (FRP), and why is it used?**
2. **Describe the process of bypassing FRP using the "Forgot Email" method.**
3. **How does the Samsung FRP Tool work for unlocking Samsung devices?**
4. **Which FRP bypass method is best for Android 8 & 9 devices?**
5. **Why does Google implement FRP security on Android devices?**

CONCLUSION

✓ FRP (Factory Reset Protection) is a Google security feature that prevents unauthorized access after a factory reset.

✓ FRP can be bypassed using account recovery, emergency call tricks, APK bypass methods, or software tools.

✓ Samsung devices require special tools like Samsung FRP Tool to bypass FRP.

✓ Technicians should only remove FRP for legitimate users who have lost access to their accounts.

Rooting & Bootloader Unlocking Methods

Understanding Rooting & Bootloader Unlocking

What is Rooting?

Rooting is the process of **gaining administrative (superuser) access** to the Android operating system, allowing users to **modify system files, remove pre-installed bloatware, and install custom ROMs**. By default, manufacturers **restrict root access** to protect the integrity and security of the device.

What is Bootloader Unlocking?

The bootloader is a **program that initializes the device hardware and loads the operating system** when the phone is powered on. Manufacturers lock the bootloader to **prevent unauthorized modifications**. Unlocking the bootloader **allows users to install custom recovery, flash custom ROMs, and root the device**.

Advantages & Risks of Rooting & Bootloader Unlocking

Advantages of Rooting & Bootloader Unlocking

✔ **Install Custom ROMs** – Replace the stock firmware with custom-built Android versions like LineageOS.

✔ **Remove Bloatware** – Uninstall unwanted pre-installed apps that slow down the device.

✔ **Improve Performance & Battery Life** – Use kernel tweaks to enhance CPU and battery efficiency.

✔ **Gain Full Control Over the OS** – Modify system files, enable hidden features, and overclock the CPU.

Risks of Rooting & Bootloader Unlocking

❌ **Voids Warranty** – Most manufacturers void the warranty if the bootloader is unlocked.
❌ **Increased Security Risks** – Root access makes the device more vulnerable to malware attacks.
❌ **Bricking the Device** – Incorrect modifications can cause the phone to **fail to boot properly (brick the phone)**.
❌ **Loss of OTA Updates** – Rooted devices may not receive official security and firmware updates.

How to Unlock the Bootloader (Step-by-Step Guide)

1. Check if the Bootloader is Unlockable

Some devices allow bootloader unlocking, while others (e.g., some Samsung and Huawei models) have permanently locked bootloaders.

✔ To check, open the **dialer** and enter the command:

fastboot oem device-info

✔ If it shows "Unlocked: No", the bootloader is locked and can be unlocked.

---

2. Enable Developer Options & OEM Unlocking

1. **Go to Settings → About Phone → Tap "Build Number" 7 times** to enable Developer Options.
2. **Navigate to Developer Options → Enable OEM Unlocking.**
3. **Enable USB Debugging** to allow communication with a PC.

3. Boot the Phone into Fastboot Mode

✓ **Power off the device.**

✓ Press and hold **Power + Volume Down** buttons simultaneously to enter **Fastboot Mode**.

4. Connect the Device to a PC & Use Fastboot Commands

1. **Install ADB & Fastboot drivers** on the PC.
2. **Open Command Prompt** and enter the following command to check if the device is detected:
3. fastboot devices
4. **Unlock the Bootloader using the following command:**
5. fastboot oem unlock
6. **Confirm Unlocking** – Some devices will display a warning message requiring user confirmation.

✓ **Outcome:** The bootloader is successfully unlocked, allowing further modifications.

Rooting Methods for Android Devices

1. Rooting Using Magisk (Recommended Method)

Magisk is the most popular rooting tool because it allows users to **gain root access without modifying the system partition**.

Steps to Root Using Magisk:

1. **Download Magisk ZIP** file and **Magisk Manager APK**.
2. **Boot the phone into custom recovery (TWRP)**.
3. **Flash the Magisk ZIP file via TWRP Recovery.**
4. **Reboot the phone and install Magisk Manager APK.**
5. **Verify root access using a root checker app.**

✓ **Outcome:** The phone is rooted while still allowing OTA updates and passing Google SafetyNet checks.

---

2. Rooting Using One-Click Root Apps (For Beginners)

Some tools like **KingRoot and iRoot** allow **one-click rooting** for devices running Android 8 and below.

✓ Steps to Root Using KingRoot:

1. **Download and install KingRoot APK.**
2. **Open the app and tap "Root".**
3. **Wait for the process to complete and reboot the device.**

✗ **Limitations:** These tools are less secure and work only on older Android versions.

---

3. Rooting by Flashing SuperSU (For Advanced Users)

SuperSU is another root management tool that allows users to **gain superuser privileges**.

✓ Steps to Root Using SuperSU:

1. **Download SuperSU ZIP file.**
2. **Boot into custom recovery (TWRP).**
3. **Flash the SuperSU ZIP file and reboot.**
4. **Verify root access using a root checker app.**

✓ **Outcome:** The device has full root privileges.

Case Study: Unlocking Bootloader & Rooting a Xiaomi Redmi Note 10

Scenario:

A user wants to install **Pixel Experience Custom ROM** on their **Xiaomi Redmi Note 10**, which requires bootloader unlocking and rooting.

Solution:

✓ **Step 1:** The user enables **OEM Unlocking** and USB Debugging.
✓ **Step 2:** Unlocks the bootloader using **Xiaomi Mi Unlock Tool**.
✓ **Step 3:** Installs **TWRP Recovery** and flashes **Magisk** to gain root access.
✓ **Step 4:** Installs **Pixel Experience ROM** and verifies root access using **Magisk Manager**.

✓ **Result:** The Xiaomi phone is now running **custom ROM with root access**.

Comparison of Rooting & Bootloader Unlocking Methods

Method	Bootloader Unlocking Required?	Risk Level	Best For
Magisk (Systemless Root)	Yes	Low	Users who want OTA updates
KingRoot (One-Click Root)	No	Medium	Beginners (older Android versions)
SuperSU (Traditional Root)	Yes	High	Advanced users

Exercise

1. **What is the main difference between rooting and bootloader unlocking?**
2. **List three advantages and three risks of rooting a phone.**
3. **Describe the step-by-step process of unlocking the bootloader on an Android phone.**
4. **Which rooting method is the most secure and widely recommended? Why?**
5. **What command is used to check bootloader unlock status via Fastboot?**

CONCLUSION

✓ Bootloader unlocking allows users to install custom recoveries, ROMs, and root their device.

✓ Rooting provides administrative control over Android but comes with security risks.

✓ Magisk is the best rooting method because it allows systemless root without affecting OTA updates.

✓ Improper rooting or bootloader unlocking can cause device bricking and void warranties.

Understanding Risks & Security Aspects of Unlocking

Introduction to Unlocking and Security Risks

Unlocking a mobile device, whether through **network unlocking, bootloader unlocking, or rooting**, provides users with **greater control over their devices**. It allows them to **switch carriers, install custom ROMs, remove bloatware, and gain administrative access**. However, unlocking also introduces **security risks, privacy concerns, and potential device instability**.

Before unlocking a device, it is crucial to understand the **associated risks and best security practices** to **protect user data, maintain device stability, and prevent unauthorized access**.

Security Risks of Network Unlocking

1. Exposure to Untrusted Networks

✓ What Happens?

- After unlocking a device from a carrier, users can switch to any network. However, not all networks **maintain strong security protocols**, increasing the risk of **man-in-the-middle attacks and data interception**.

✓ Example:

- A user unlocks a **T-Mobile device** and switches to a **low-cost carrier** with weaker encryption standards. The user’s calls and messages may be more susceptible to interception.

✓ Mitigation Strategy:

- Use **VPN services** and **encrypted communication apps (Signal, WhatsApp)** to secure network communications.

---

2. Increased Risk of SIM Swapping Attacks

✓ What Happens?

- Once a phone is **network unlocked**, it can use **multiple SIM cards**. If an attacker gains access to a user's SIM, they can **hijack calls, messages, and even financial transactions**.

✓ Example:

- A hacker tricks the mobile carrier into transferring a user's phone number to a new SIM card, gaining access to **banking OTPs, emails, and social media accounts**.

✓ Mitigation Strategy:

- Use **two-factor authentication (2FA) with authenticator apps** instead of SMS-based authentication.
- Contact the carrier to **enable SIM card PIN protection**.

RISKS OF BOOTLOADER UNLOCKING

1. Increased Risk of Malware & Unauthorized Modifications

✓ What Happens?

- A locked bootloader ensures that only **signed firmware** can run on the device. Unlocking the bootloader allows **unverified software** to be installed, increasing the risk of **malware injection and unauthorized system modifications**.

✓ Example:

- A user installs a **custom ROM** from an untrusted source. The ROM contains a **hidden keylogger**, which records keystrokes and sends user credentials to hackers.

✓ Mitigation Strategy:

- Only **download firmware and custom ROMs from trusted sources (LineageOS, Pixel Experience, XDA Developers)**.
- Verify ROM integrity using **checksums (SHA256, MD5)** before flashing.

---

2. Voiding Manufacturer Warranty

✓ What Happens?

- Many manufacturers **void the warranty** once the bootloader is unlocked, meaning users **cannot claim free repairs** if issues arise.

✓ Example:

- A user unlocks the bootloader to install a **custom kernel** but experiences **overheating and battery drain**. When they approach the service center for repairs, the manufacturer **refuses service due to the unlocked bootloader**.

✓ Mitigation Strategy:

- Some brands like **OnePlus and Google** allow **warranty claims even after unlocking**. Check the manufacturer's policy before unlocking.

- Use **fastboot relock commands** to restore the bootloader to a locked state before claiming warranty.

---

3. Increased Risk of Device Bricking

✓ What Happens?

- A bricked device becomes **completely unresponsive**, often due to **flashing incompatible firmware, kernel modifications, or incorrect system commands**.

✓ Example:

- A user attempts to root a **Samsung device** by flashing a kernel designed for a different model. The phone **fails to boot, and recovery mode is inaccessible**, causing a **hard brick**.

✓ Mitigation Strategy:

- Always **back up the stock ROM** before modifying system files.
- Use manufacturer-provided tools (**Samsung Odin, QPST, SP Flash Tool**) for proper firmware restoration.

Risks of Rooting a Device

1. Loss of Google SafetyNet & Banking App Restrictions

✓ What Happens?

- Many apps rely on **Google SafetyNet** to ensure that the device is running **secure, unmodified firmware**. Rooting **breaks SafetyNet**, restricting access to **banking apps, Netflix, and Google Pay**.

✓ **Example:**

- A user roots their device to install **ad-blocking software**. Later, they discover that **Google Pay and their banking app refuse to work**.

✓ **Mitigation Strategy:**

- Use **Magisk (systemless root)** to hide root access from apps.
- Use the **Magisk Hide feature** to bypass SafetyNet checks.

---

2. Exposure to Advanced Persistent Threats (APTs) & Remote Attacks

✓ **What Happens?**

- Rooting allows apps to **modify system files**. A malicious app with root permissions can install **spyware, steal sensitive data, or remotely control the device**.

✓ **Example:**

- A user downloads a **modded app** from an untrusted source. The app requests root access and **silently installs a trojan that sends personal data to hackers**.

✓ **Mitigation Strategy:**

- Only grant root access to **trusted apps**.
- Use **root management apps (Magisk Manager, SuperSU)** to monitor app permissions.

Scenario:

A technician receives a **OnePlus 8T** from a customer who unlocked the bootloader and installed a custom ROM. The customer complains that:

1. **Google Pay is not working.**
2. **Their banking app refuses to open.**
3. **The device is slower and experiencing random reboots.**

Solution:

✓ **Step 1:** Checked system logs and confirmed that **SafetyNet failed due to bootloader unlocking**.
✓ **Step 2:** Installed **Magisk** to pass SafetyNet and enable banking apps.
✓ **Step 3:** Restored the stock kernel to fix stability issues.
✓ **Step 4:** Advised the customer about **security risks and warranty policies**.

✓ **Result:** The phone **retained root access but was secured** against SafetyNet restrictions, improving functionality.

Comparison of Unlocking Methods & Security Risks

Method	Risk Level	Common Security Issues	Mitigation Strategy
Network Unlocking	Medium	SIM Swapping, Network Vulnerabilities	Use VPN & 2FA

Bootloader Unlocking	High	Malware Injection, Warranty Void	Verify ROM Integrity
Rooting	Very High	Banking Apps Blocked, Remote Hacking	Use Magisk & Trusted Apps

---

Exercise

1. **What are the security risks associated with network unlocking?**
2. **Explain why unlocking the bootloader increases malware risks.**
3. **Describe three best practices to secure a rooted device.**
4. **How does Google SafetyNet affect rooted devices?**
5. **Why do manufacturers void warranties for unlocked bootloaders?**

Conclusion

✓ Unlocking provides freedom but introduces security vulnerabilities.

✓ Network unlocking can expose devices to SIM swapping and weak security networks.

✓ Bootloader unlocking makes devices susceptible to malware, warranty loss, and bricking.

✓ Rooting increases hacking risks but can be managed using Magisk and secure permissions.

ASSIGNMENT 3:

✓ DEMONSTRATE UNLOCKING A TEST DEVICE USING DIFFERENT METHODS (FRP BYPASS, BOOTLOADER UNLOCK).

✓ EXPLAIN THE SECURITY RISKS INVOLVED IN UNAUTHORIZED UNLOCKING.

Demonstration: Unlocking a Test Device Using Different Methods (FRP Bypass, Bootloader Unlock)

Unlocking a mobile device involves **removing restrictions set by manufacturers or software** to allow deeper access and modifications. The two main types of unlocking are:

✓ **FRP Bypass (Factory Reset Protection Removal)** – Used to regain access to a phone that is locked due to a factory reset without the original Google account credentials.
✓ **Bootloader Unlocking** – Required for **installing custom ROMs, gaining root access, and modifying system files**.

This guide demonstrates step-by-step **how to unlock a test device using both FRP Bypass and Bootloader Unlocking methods**.

Method 1: Bypassing Google FRP Lock (Factory Reset Protection)

Scenario

A **Samsung Galaxy A51** is factory reset, but the user forgets their Google account credentials. The phone is stuck on the **Google verification screen**, asking for the original account details.

Method 1: Using FRP Bypass APK (For Android 8 & Above)

Step 1: Connect to Wi-Fi & Open the Google Verification Page

- Turn on the locked device and **connect to Wi-Fi**.
- Reach the **Google Account Verification** screen.

Step 2: Access Chrome Browser via YouTube Trick

- On the Google Verification page, **tap & hold the "@" symbol** on the keyboard.
- Select **Google Keyboard Settings → Help & Feedback → Use Morse Code**.

- A YouTube video opens. Click **Share → Open in Chrome**.

Step 3: Download & Install FRP Bypass APK

- In Chrome, search for **“FRP Bypass APK”** and download it.
- Enable **Unknown Sources** in Chrome settings.
- Install and open **FRP Bypass APK**.

Step 4: Remove Google Account & Restart the Device

- In FRP Bypass, **tap "Bypass FRP" → Open Settings → Accounts**.
- Remove the **existing Google account** and reboot the device.

✓ **Outcome:** The phone bypasses FRP and allows the user to add a new Google account.

Method 2: Using Samsung FRP Tool (For Samsung Devices Only)

Step 1: Install Samsung FRP Tool on PC

- Download **Samsung FRP Tool** on a Windows PC.
- Connect the locked Samsung device to the PC via USB.

Step 2: Enable ADB Mode & Remove FRP Lock

- Open **Samsung FRP Tool** and select **"Bypass FRP"**.
- The tool will send an **ADB command to the phone**.
- The phone will automatically **restart** and FRP will be removed.

✓ **Outcome:** The Samsung device is now FRP-unlocked and ready for use.

Method 2: Unlocking the Bootloader

Scenario

A technician wants to unlock the bootloader on a **OnePlus 8T** to install a **custom ROM (LineageOS)**.

Step 1: Enable Developer Options & OEM Unlocking

- Go to **Settings → About Phone**.
- Tap **“Build Number” 7 times** to enable Developer Mode.
- Navigate to **Developer Options → Enable OEM Unlocking & USB Debugging**.

Step 2: Boot the Device into Fastboot Mode

- Power off the phone.
- Press & hold **Power + Volume Down** to enter **Fastboot Mode**.
- Connect the phone to a PC using a USB cable.

Step 3: Unlock Bootloader Using Fastboot Commands

- Install **ADB & Fastboot drivers** on the PC.
- Open **Command Prompt (CMD)** and enter:
- fastboot devices

(This ensures the device is detected in Fastboot mode.)

- Enter the following command to unlock the bootloader:
- fastboot oem unlock
- The phone will show a warning screen. Use **Volume Up** to confirm.

Step 4: Reboot & Verify Bootloader Status

- Enter the command:

- fastboot reboot
- To check if the bootloader is unlocked, use:
- fastboot oem device-info

✓ **Outcome:** The OnePlus 8T now has an **unlocked bootloader**, allowing custom ROM installations and rooting.

Comparison of Unlocking Methods

Method	Used For	Best For	Risk Level	Outcome
FRP Bypass (APK Trick)	Removing Google FRP Lock	Android 8+ Devices	Medium	Allows new Google Account login
Samsung FRP Tool	Removing FRP on Samsung	Samsung Phones	Low	Removes Google Account Verification
Bootloader Unlocking (Fastboot)	Installing Custom ROMs & Rooting	OnePlus, Xiaomi, Google Phones	High	Allows Custom ROM & Root Access

Case Study: FRP Bypass & Bootloader Unlock on a Xiaomi Redmi Note 10

Scenario:

A customer wants to unlock their **Redmi Note 10**, which is stuck on FRP lock after a factory reset. Later, they also want to install **Pixel Experience ROM**, which requires bootloader unlocking.

Solution:

✓ **Step 1:** Bypassed FRP using **FRP Bypass APK Trick**.
✓ **Step 2:** Unlocked the bootloader using **Xiaomi Mi Unlock Tool**.
✓ **Step 3:** Installed **TWRP Recovery** and flashed **Pixel Experience ROM**.
✓ **Step 4:** Verified device stability and root access.

✓ **Result:** The Redmi Note 10 is **fully unlocked and running a custom ROM**.

Exercise

1. **What is the purpose of FRP Lock, and why does Google implement it?**
2. **Explain how to use the FRP Bypass APK method to unlock a device.**
3. **List the steps to unlock the bootloader of an Android device using Fastboot commands.**
4. **Why is bootloader unlocking required before installing a custom ROM?**
5. **Describe the risks associated with unlocking a bootloader.**

CONCLUSION

✓ **FRP Bypass allows users to regain access to factory-reset devices without the original Google account.**
✓ **Bootloader unlocking provides the freedom to install custom ROMs and modify system files.**
✓ **Samsung FRP Tool is an effective method for bypassing FRP on Samsung phones.**
✓ **Fastboot commands are essential for unlocking bootloaders on OnePlus, Xiaomi, and Pixel devices.**

Security Risks Involved in Unauthorized Unlocking (Step-by-Step Guide)

Unauthorized unlocking of mobile devices—including **network unlocking, bootloader unlocking, and FRP bypassing**—can expose users to **serious security risks**. While unlocking offers flexibility, it also **removes critical security layers**, making the device vulnerable to **data theft, malware, hacking, and unauthorized access**.

This guide explains **the key security risks** involved in unauthorized unlocking and provides **a step-by-step breakdown of how each risk occurs, along with best practices to mitigate them**.

Step 1: Understanding Unauthorized Unlocking

What is unauthorized unlocking?
Unauthorized unlocking refers to any process that removes security restrictions **without proper authorization or legal permission**. This includes:

✓ **Bypassing Factory Reset Protection (FRP)** – Removing Google account verification after a factory reset.
✓ **Bootloader Unlocking without Permission** – Unlocking a locked bootloader **without manufacturer approval**.
✓ **Illegal IMEI Changing** – Altering a device's IMEI to **avoid tracking or network restrictions**.
✓ **Carrier Unlocking without Authorization** – Removing a carrier lock **without approval from the original network provider**.

While these methods enable **customization and flexibility**, they **also pose serious security threats**.

Step 2: Common Security Risks of Unauthorized Unlocking

1. Increased Vulnerability to Malware & Hacking

✓ How it Happens:

- Unlocking the bootloader removes security protections, allowing **unsigned or malicious software** to be installed.
- Rooted devices can execute **unauthorized background processes**, making them more susceptible to **remote hacking**.

✓ Example:

- A user downloads a **modified banking app** from an untrusted website.
- The app requests root access and silently **steals login credentials**.

✓ Mitigation Strategy:

- Only install **trusted applications** from official sources (Google Play Store, F-Droid).
- Use **Magisk Hide** to prevent banking apps from detecting root access.

---

2. Exposure to SIM Cloning & SIM Swap Attacks

✓ How it Happens:

- Unauthorized network unlocking removes carrier restrictions, allowing users to **insert any SIM card**.
- Attackers exploit this by **cloning SIM cards** or **convincing the carrier to transfer the victim's number** to a new SIM.

✓ Example:

- A hacker gains access to a user's **phone number and personal information**.
- They use a SIM swap attack to **hijack two-factor authentication (2FA) SMS codes** and access **bank accounts, emails, and social media**.

✓ Mitigation Strategy:

- **Use authenticator apps (Google Authenticator, Authy) instead of SMS-based 2FA.**
- Contact your carrier to enable **SIM card PIN protection**.

---

3. Permanent Device Bricking

✓ How it Happens:

- Modifying critical system files or flashing **incompatible firmware** can result in a **hard brick**, rendering the device unusable.
- Certain manufacturers **block bootloader unlocking**, making **improper flashing** irreversible.

✓ Example:

- A user tries to install **a custom kernel on a Samsung Galaxy phone**.
- The phone **fails to boot, and recovery mode is inaccessible**, leading to **a permanently bricked device**.

✓ Mitigation Strategy:

- Always **backup the stock firmware** before unlocking or flashing.
- Use manufacturer-approved tools (**Samsung Odin, QPST, SP Flash Tool**) for recovery.

---

4. Loss of Manufacturer Warranty & OTA Updates

✓ How it Happens:

- Many phone manufacturers **void the warranty** once the bootloader is unlocked or the device is rooted.
- Rooting disables **official OTA updates**, preventing users from receiving **critical security patches**.

✓ Example:

- A user **unlocks the bootloader on a OnePlus device** to install a custom ROM.
- The device develops a **hardware fault, but the service center refuses to repair it** due to **warranty voidance**.

✓ **Mitigation Strategy:**

- Before unlocking, check **manufacturer policies** regarding bootloader unlocking and warranty coverage.
- Some devices (**Google Pixel, OnePlus**) allow **relocking the bootloader** before claiming warranty.

---

5. Increased Risk of Data Theft & Identity Fraud

✓ **How it Happens:**

- Unauthorized unlocking techniques often **disable factory reset protection (FRP)**, allowing **stolen devices** to be resold without restrictions.
- Some fraudulent unlocking methods involve **sharing IMEI numbers with third-party services**, which can lead to **identity theft**.

✓ **Example:**

- A user buys a second-hand **iPhone that was FRP-bypassed using third-party software**.
- Later, Apple **blacklists the device as stolen**, making it **unusable on any network**.

✓ **Mitigation Strategy:**

- Always **buy unlocked devices from authorized sellers**.
- Before purchasing a used phone, check its **IMEI status using websites like IMEI.info** to confirm it is not blacklisted.

Step 3: Best Practices to Secure an Unlocked Device

If unlocking is necessary, follow these security best practices:

✓ **Use Trusted Unlocking Methods** – Follow **official unlocking procedures** provided by manufacturers (OnePlus, Google, Samsung).
✓ **Enable Full-Disk Encryption** – Protects data even if the device is unlocked or rooted.
✓ **Use a Strong Screen Lock & Biometrics** – Adds an extra security layer to prevent unauthorized access.
✓ **Install Security Updates Manually** – If OTA updates are disabled, manually flash security patches from trusted sources.
✓ **Avoid Storing Sensitive Information on Rooted Devices** – Prevents **data breaches in case of malware infection**.

Case Study: Unauthorized Unlocking Leads to Security Breach

Scenario:

A customer unlocks the **bootloader on their Xiaomi phone** to install a custom ROM. However, they later:

1. **Lose access to banking apps because SafetyNet fails.**
2. **Download a third-party firmware update from an untrusted source.**
3. **Experience unauthorized data transfers** and suspect malware.

Solution:

✓ **Step 1:** Re-installed a verified custom ROM (**LineageOS**) from a **trusted source**.
✓ **Step 2:** Used **Magisk Hide** to pass SafetyNet and restore banking app functionality.
✓ **Step 3:** Enabled **firewall protection (AFWall+)** to block unknown network connections.

✓ **Result:** The device is **secure and free from malware** while still retaining **custom ROM functionality**.

Exercise

1. **What are the security risks of unlocking the bootloader?**
2. **Why does unauthorized FRP bypass increase the chances of stolen devices being resold?**
3. **Explain how SIM swap attacks occur and how to prevent them.**
4. **What steps should a user take to minimize security risks after unlocking a device?**
5. **Describe the impact of unauthorized IMEI changes on mobile security.**

Conclusion

✓ Unauthorized unlocking increases security vulnerabilities, including malware risks, SIM swap attacks, and data theft.

✓ Bootloader unlocking disables critical security features, leaving devices exposed to unauthorized modifications.

✓ Unauthorized FRP bypassing is often used for illegal activities and weakens mobile theft protection.

✓ Users should take extra precautions, such as using Magisk, trusted unlocking tools, and full-disk encryption.