# Mobile Device Security

Contents

[Mobile Device Security 1](#_Toc182127655)

[Understanding App Permissions 1](#_Toc182127656)

[Location Tracking and Geofencing 2](#_Toc182127657)

[Handling Failed Login Attempts 2](#_Toc182127658)

[Secure Authentication Practices 2](#_Toc182127659)

[Password Management 3](#_Toc182127660)

[Network Security 3](#_Toc182127661)

[Physical Security 4](#_Toc182127662)

[Emergency Response Plan 4](#_Toc182127663)

[General Mobile Device Security Best Practices 5](#_Toc182127664)

[Key Takeaways 5](#_Toc182127665)

[Assignment Reflection 5](#_Toc182127666)

[Assignment Submission 6](#_Toc182127667)

Time required: 60 minutes

In this tutorial, we’ll cover essential security practices for mobile devices, focusing on protecting personal data and preventing unauthorized access. The content is divided into sections on app permissions, location tracking, failed login responses, authentication methods, and general best practices.

# Understanding App Permissions

Limit what apps can access on your device to prevent data misuse.

* **Review Permissions Regularly**: Periodically check app permissions in your device settings. Remove access to sensitive information like location, contacts, or storage when unnecessary.

**Insert a screenshot showing the app permission for one app.**

Click or tap here to enter text.

* **Beware of Default Permissions**: Many apps request more permissions than needed. Grant only those permissions essential for the app’s core functions.
* **Limit Location Access**: Only allow location access for apps that require it (e.g., maps). Choose “While Using App” rather than “Always” where possible.

**Tip**: On Android, navigate to Settings > Apps > to review and adjust app permissions. On iOS, go to Settings > Privacy > Location Services.

# Location Tracking and Geofencing

Control how apps and services use your location data.

* **Use Built-in Security Options**: Both Android and iOS offer location permissions that allow apps to access your location only while actively in use.
* **Enable Geofencing Carefully**: Some apps use geofencing to automate actions based on location. Use it cautiously, as it can be exploited for tracking.
* **Disable Background Location Access**: If apps can track your location in the background, they may be able to record your movements over time.

**Tip**: To disable background tracking on Android, go to Settings > Location > App Permissions. On iOS, go to Settings > Privacy > Location Services.

# Handling Failed Login Attempts

Protect accounts and data from brute force attacks or unauthorized access.

* **Account Lockouts**: Configure lockouts after several failed attempts to prevent brute force attacks. Most apps allow account locking or require a captcha.
* **Alerts for Failed Logins**: Many apps can send alerts when a failed login attempt occurs. Use these to detect suspicious activity.
* **Two-Factor Authentication (2FA)**: Enable 2FA for sensitive apps (like banking). This adds an extra layer of security if a password is compromised.

**Tip**: Lockouts after 3–5 failed attempts and alert notifications provide early warning against unauthorized access.

# Secure Authentication Practices

Use strong, secure authentication to prevent unauthorized access.

* **Use Biometric Authentication**: Fingerprint or facial recognition are highly secure. They offer better protection than traditional PINs.
* **Implement Strong Passwords**: Choose long, complex passwords and avoid reusing them. Password managers help store and generate strong passwords.
* **Enable Multifactor Authentication (MFA)**: MFA combines something you know (password) with something you have (like a code sent to your phone). This is critical for securing apps containing sensitive data.

**Tip**: Avoid using PINs shorter than 6 digits, and consider biometric options for both convenience and security.

**Insert a screenshot of an MFA application on your phone showing the accounts**.

Click or tap here to enter text.

# Password Management

* Use a password manager
* Generate unique passwords for each account
* Regular password changes for critical accounts
* Never store passwords in notes/contacts

# Network Security

**Wi-Fi Safety**

* Avoid public Wi-Fi when possible
* Use VPN on public networks
* Disable auto-connect to Wi-Fi networks
* Forget networks you no longer use

**Show your wireless networks and how to forget a network.**

Click or tap here to enter text.

* Disable Wi-Fi when not in use

**Bluetooth Security**

* Disable Bluetooth when not in use
* Use "hidden" mode when possible
* Regularly remove paired devices you no longer use
* Never pair devices in public places

# Physical Security

**Device Protection**

* Use a quality protective case
* Apply screen protector
* Never leave device unattended
* Use lockable storage when needed

# Emergency Response Plan

**If Device is Lost/Stolen**

1. Immediately lock device remotely
2. Change critical passwords
3. Contact carrier to disable service
4. Report to appropriate authorities
5. Activate remote wipe if necessary

**If Device is Compromised**

1. Disconnect from network
2. Back up essential data
3. Factory reset device
4. Change all passwords
5. Restore from clean backup

# General Mobile Device Security Best Practices

* **Keep Your OS and Apps Updated**: Updates often patch security vulnerabilities. Turn on automatic updates if available.

**Insert a screenshot showing your update status.**

Click or tap here to enter text.

* **Install Apps Only from Trusted Sources**: Download apps from official stores (Google Play or Apple App Store) to minimize malware risk.
* **Use a Secure VPN on Public Wi-Fi**: Public Wi-Fi networks are unprotected, making you vulnerable to data interception. Use a VPN to secure your connection.
* **Enable Find My Device**: In case your device is lost or stolen, enable tracking features like Find My Device (Android) or Find My iPhone (iOS).

**Insert a screenshot showing your phone location**.

Click or tap here to enter text.

* **Regularly Back Up Data**: Back up data to a secure cloud service or computer in case of loss, theft, or damage.

**Insert a screenshot showing your mobile device backup status**

Click or tap here to enter text.

# Key Takeaways

* **Control App Permissions**: Review permissions, especially for location, contacts, and storage.
* **Enable Failed Login Alerts**: Detect suspicious activity early with failed login notifications.
* **Adopt Secure Authentication**: Use strong passwords, biometric options, and MFA whenever possible.
* **Use Built-in Security Tools**: Keep your device updated, back up data, and activate lost-device tracking.

# Assignment Reflection

Reflect on your findings.

* What did you learn about mobile device security that you didn’t know before?
  + How can you apply this knowledge to your own devices?

|  |
| --- |
| Click or tap here to enter text. |

## Assignment Submission

* Attach this completed document to the assignment in Blackboard.