Cyber Security - Report

Comprehensive Mobile Security & Social Media Privacy Checklist

- M. Jonah Paulin Joyce - 241051004018
- Samyuktaa SV - 241051004008

Mobile security is crucial in today's digital age. Here's a checklist of 10 best practices to keep your mobile device secure, along with detailed explanations and a social media privacy review.

10 Best Practices for Mobile Security

1. **Use Strong, Unique Passwords/PINs:**
    - **Explanation:** Your lock screen is the first line of defense. A strong password (alphanumeric, special characters) or a complex PIN (6+ digits, not easily guessable) makes it harder for unauthorized users to access your device.
    - **Demonstration (General Steps for Android/iOS):**
        - Go to **Settings**.
        - Navigate to **Security & privacy** (Android) or **Face ID & Passcode / Touch ID & Passcode** (iOS).
        - Select **Screen lock** (Android) or **Change Passcode** (iOS).
        - Choose a strong password, PIN, or pattern, and confirm it.

2. **Enable Biometric Locks (Fingerprint/Face Recognition):**
    - **Explanation:** Biometric authentication provides a convenient and often more secure way to unlock your device. It's harder to spoof than a simple

PIN.

- **Demonstration (General Steps for Android/iOS):**
  - Go to **Settings**.
  - Navigate to **Security & privacy** (Android) or **Face ID & Passcode / Touch ID & Passcode** (iOS).
  - Select **Fingerprint** or **Face Recognition** (Android) or **Set Up Face ID / Add a Fingerprint** (iOS).
  - Follow the on-screen instructions to register your biometrics.
- `

3. **Review App Permissions Regularly:**
   - **Explanation:** Apps often request access to your camera, microphone, location, contacts, and storage. Granting unnecessary permissions can compromise your privacy and security. Regularly review and revoke permissions that aren't essential for the app's functionality.
   - **Demonstration (General Steps for Android/iOS):**
     - Go to **Settings**.
     - Navigate to **Apps & notifications** then **App permissions** (Android) or **Privacy & Security** then **Permission Manager** (Android) or **Privacy** (iOS).
     - Tap on a specific permission (e.g., Location, Camera) to see which apps have access, and toggle off access for those that don't need it.
     - Alternatively, go to a specific app's settings and manage its permissions.
   - `

4. **Avoid Unofficial APKs and App Stores:**
   - **Explanation:** Sideloading apps from third-party sources (unofficial APKs) bypasses the security checks of official app stores (Google Play Store, Apple App Store). These unofficial apps can contain malware, viruses, or spyware.

   - **Step-by-step Process:**
      - **Always download apps from official sources.**
      - On Android, go to **Settings > Apps & notifications > Special app access > Install unknown apps** and ensure that "Allow from this source" is disabled for all browsers or messaging apps you don't explicitly trust for app downloads.
      - iOS generally restricts sideloading, making it inherently safer in this regard.
   - `

5. **Keep Your Operating System and Apps Updated:**
   - **Explanation:** Software updates often include critical security patches that fix vulnerabilities. Keeping your OS and apps up-to-date helps protect your device from the latest threats.
   - **Demonstration (General Steps for Android/iOS):**
      - **OS Update:** Go to **Settings > System > System update** (Android) or **Settings > General > Software Update** (iOS).
      - **App Updates:**
         - **Android:** Open Google Play Store, tap your profile icon, then **Manage apps & device**, then **Update all**.
         - **iOS:** Open App Store, tap your profile icon, then scroll down to see pending updates.
   - `

6. **Enable Two-Factor Authentication (2FA) Wherever Possible:**
   - **Explanation:** 2FA adds an extra layer of security by requiring a second verification method (like a code sent to your phone or generated by an authenticator app) in addition to your password.
   - **Step-by-step Process (General):**
      - Whenever you set up an online account, look for a "Security" or "Privacy" section in its settings.

        - Enable "Two-Factor Authentication" or "Two-Step Verification."
        - Choose your preferred method (SMS, authenticator app, security key).
        - For your Google account on Android, go to **Settings > Google > Manage your Google Account > Security > 2-Step Verification**.
        - For Apple ID on iOS, go to **Settings > [Your Name] > Password & Security > Two-Factor Authentication**.
    - `

7. **Use a VPN on Public Wi-Fi:**
    - **Explanation:** Public Wi-Fi networks are often unsecured and can be easily intercepted by malicious actors. A Virtual Private Network (VPN) encrypts your internet traffic, protecting your data from prying eyes.
    - **Step-by-step Process:**
        - Download and subscribe to a reputable VPN service.
        - Install the VPN app on your mobile device.
        - Open the VPN app and connect to a server before using public Wi-Fi.
    - `

8. **Be Wary of Phishing Attempts:**
    - **Explanation:** Phishing is a common social engineering tactic where attackers try to trick you into revealing sensitive information (passwords, credit card numbers) by impersonating legitimate entities via email, text, or calls.
    - **Tips:**
        - **Check the sender:** Look for suspicious email addresses or phone numbers.
        - **Look for red flags:** Poor grammar, unusual requests, urgent language.
        - **Don't click suspicious links:** Hover over links to see the actual URL before clicking.

    - **Verify directly:** If you receive a suspicious request from a company, contact them directly through their official website or phone number.
- `

9. **Encrypt Your Device:**
    - **Explanation:** Device encryption scrambles all the data on your phone, making it unreadable to anyone who doesn't have the decryption key (usually your lock screen password/PIN). Most modern Android and iOS devices are encrypted by default.
    - **Demonstration (General Steps):**
        - **Android:** Go to **Settings > Security & privacy > Encryption & credentials**. If your device isn't encrypted, you'll see an option to encrypt it. Newer Android devices are typically encrypted by default.
        - **iOS:** iPhones and iPads are encrypted by default with hardware-based encryption once a passcode is set.
    - `

10. **Regularly Back Up Your Data:**
    - **Explanation:** In case your device is lost, stolen, or damaged, having a recent backup ensures you don't lose your important photos, contacts, and documents.
    - **Demonstration (General Steps for Android/iOS):**
        - **Android (Google Drive):** Go to **Settings > Google > Backup** and ensure "Backup by Google One" is turned on. You can also manually initiate a backup.
        - **iOS (iCloud):** Go to **Settings > [Your Name] > iCloud > iCloud Backup** and ensure it's toggled on. You can also tap "Back Up Now."
    - `

Social Media Privacy Review: Instagram

Instagram is a widely used social media platform. Here's how to review and manage your privacy settings to limit data sharing, manage followers/friend requests, and avoid impersonation.

Step-by-step Process for Instagram Privacy Settings:

1. **Access Settings:**
    - Open the Instagram app.
    - Tap on your **profile picture** in the bottom right corner.
    - Tap the **three horizontal lines** (menu icon) in the top right corner.
    - Tap **Settings and privacy**.
    - `
2. **Account Privacy (Private Account):**
    - **Explanation:** Making your account private means only approved followers can see your posts, stories, and Reels. This is the most fundamental privacy setting.
    - **How to Limit Data Sharing/Manage Followers:**
        - From **Settings and privacy**, tap **Account privacy**.
        - Toggle on **Private Account**.
        - **Managing Follow Requests:** When your account is private, new followers will send a "Follow Request" that you must approve or decline.
            - Go to your **profile**, tap on **Follower requests**.
            - Review pending requests and tap **Confirm** or **Delete**.
        - `
3. **Manage Who Can See Your Content:**
    - **Blocked Accounts:**
        - **Explanation:** Blocked users cannot find your profile, posts, or send you messages.
        - **How to Block:**
            - Go to the profile of the user you want to block.

        - Tap the **three dots** in the top right corner.
        - Tap **Block**.
    - You can manage your blocked accounts by going to **Settings and privacy > Blocked accounts**.
- `
- **Hide Story and Live from:**
    - **Explanation:** You can prevent specific followers from seeing your Instagram Stories and Live videos.
    - **How to use:**
        - From **Settings and privacy**, scroll down to "Who can see your content" section, tap **Hide story and live from**.
        - Select the users you want to hide your stories/live from.
    - `
- **Close Friends:**
    - **Explanation:** Share your stories only with a select group of people.
    - **How to use:**
        - From **Settings and privacy**, tap **Close Friends**.
        - Add or remove people from your close friends list. When creating a story, you'll have the option to share it only with Close Friends.
    - `

4. **Interactions (Managing Comments, Tags, Mentions):**

- **Comments:**
    - **Explanation:** Control who can comment on your posts and filter out unwanted comments.
    - **How to manage:**
        - From **Settings and privacy**, scroll down to "How others can interact with you" section, tap **Comments**.

        - You can "Allow comments from" specific groups (Everyone, People you follow and your followers, People you follow, Your followers).
        - You can also toggle on **Hide offensive comments** or manually enter **Manual Filters** for specific words or phrases.
    - `
- **Tags and Mentions:**
    - **Explanation:** Prevent others from tagging or mentioning you without your approval, which helps avoid unwanted visibility and potential impersonation.
    - **How to manage:**
        - From **Settings and privacy**, tap **Tags and mentions**.
        - Under "Who can tag you," choose between "Everyone," "People you follow," or "No One."
        - Toggle on **Manually approve tags** for more control.
        - Under "Who can mention you," choose between "Everyone," "People you follow," or "No One."
    - `

5. **Messages and Story Replies:**
    - **Explanation:** Control who can send you direct messages and reply to your stories.
    - **How to manage:**
        - From **Settings and privacy**, tap **Messages and story replies**.
        - You can set controls for "Message Controls" (e.g., who can add you to groups) and "Story Replies" (e.g., allow replies from Everyone, People you follow, or turn off).
        - `
6. **Data Usage and Permissions:**

- **Explanation:** Review how Instagram uses your data and the permissions it has on your device.
- **How to manage:**
    - On your phone's **System Settings** (not Instagram settings), go to **Apps** (Android) or **Instagram** (iOS).
    - Tap **Permissions** (Android) or **Photos/Camera/Location/Microphone** (iOS).
    - Review and revoke any unnecessary permissions (e.g., if you don't post from your location, turn off location access for Instagram).
    - On Instagram itself, under **Settings and privacy**, look for sections like **Account Center** (Meta accounts) or **Your activity** where you might see options related to data and privacy.
- `

Avoiding Impersonation on Instagram:

1. **Enable Two-Factor Authentication (2FA):**
    - **Explanation:** As mentioned in general mobile security, 2FA is critical for Instagram. It prevents unauthorized access even if someone gets your password.
    - **How to enable:**
        - From **Settings and privacy**, tap **Account Center**.
        - Tap **Password and security**.
        - Tap **Two-factor authentication** and follow the prompts to set it up (via authentication app, WhatsApp, or SMS).
    - `
2. **Strong, Unique Password:**
    - **Explanation:** Use a complex password not reused on other sites.
    - **How to change:**
        - From **Settings and privacy**, tap **Account Center**.

    - Tap **Password and security**.
    - Tap **Change password**.
- `

3. **Be Cautious of Phishing Attempts:**
    - **Explanation:** Instagram scammers often send fake emails or DMs asking for your login credentials. Instagram will never ask for your password via email or DM.
    - **Tips:** Always verify the sender and URL before clicking any links or providing information.
    - `
4. **Monitor for Suspicious Activity:**
    - **Explanation:** Regularly check your "Login Activity" to see where your account has been accessed.
    - **How to check:**
        - From **Settings and privacy**, tap **Account Center**.
        - Tap **Password and security**.
        - Tap **Where you're logged in**. Log out of any unfamiliar devices.
    - `
5. **Report Impersonation:**
    - **Explanation:** If you find an account impersonating you or someone you know, report it to Instagram immediately.
    - **How to report:**
        - Go to the impersonating profile.
        - Tap the **three dots** in the top right corner.
        - Tap **Report**.
        - Select "It's inappropriate" then "Pretending to be someone else" and follow the prompts.

- `

By diligently following these mobile security best practices and regularly reviewing your social media privacy settings, you can significantly enhance your digital safety and protect your personal information.