Mobile Banking Security Checklist

REVIEW: Take a few minutes to review this checklist.

CUSTOMIZE: While this checklist covers essential security measures, some may be specific to your bank's app. Familiarize yourself with your bank's security features for a more comprehensive approach.

SECURING YOUR DEVICE:

- **Strong Passcode/Fingerprint/Face ID:** Enable a strong passcode, fingerprint scan, or facial recognition for your phone's security.
- **Operating System Updates:** Keep your phone's operating system updated with the latest security patches.
- **Mobile Security Software:** Consider reputable mobile security software to add an extra layer of protection.

SECURING YOUR MOBILE BANKING APP:

- **Official App Store:** Download your mobile banking app only from the official app store (e.g., Apple App Store, Google Play Store).
- **Strong Password/PIN:** Create a strong, unique password or PIN for your mobile banking app (different from your phone's unlock code).
- **Two-Factor Authentication (2FA):** Enable 2FA for your mobile banking app if available. This adds an extra verification step during login.
- **App Updates:** Update your mobile banking app regularly to ensure you have the latest security features.
- **Security Settings:** Explore the security settings within your mobile banking app and enable features like auto-lock or requiring a PIN after a period of inactivity.
- **Permissions:** Review and adjust permissions granted to your mobile banking app. Only allow access to features essential for the app's functionality.

SAFE MOBILE BANKING HABITS:

- **Avoid Public Wi-Fi:** For sensitive transactions like mobile banking, use a secure, private network (e.g., your home Wi-Fi).
- **Be Cautious with Information:** Don't share sensitive information like passwords or account details via email, text message, or phone calls unless you initiated contact with your bank directly.
- **Beware of Phishing Scams:** Be suspicious of unsolicited emails, text messages, or calls claiming to be from your bank. Never click on links or download attachments from unknown senders.
- **Monitor Accounts Regularly:** Review your bank statements and transaction history regularly for any suspicious activity.
- **Enable Bank Alerts:** Consider enabling account alerts for transactions, login attempts, or large withdrawals to stay informed of any unusual activity.

IN CASE OF EMERGENCY:

- **Lost/Stolen Phone:** Contact your bank immediately to report a lost or stolen phone and request them to secure your accounts. Utilize remote wipe features on your phone if available.
- **Suspected Security Breach:** If you suspect a security breach (unauthorized transactions, compromised login), contact your bank immediately and report the issue to freeze your account.
- **Use Remote Wiping Features**: If your phone is lost or stolen, use remote wiping features to erase your data.

ADDITIONAL TIPS:

- **Use a VPN for an extra layer of security on public Wi-Fi (optional).**
- **Change your passwords periodically, especially if you suspect a compromise.**
- **Consider using a password manager to create and manage strong, unique passwords for all your online accounts.**

REMEMBER:

- Stay informed about the latest mobile banking threats.
- Contact your bank if you have any questions or concerns about mobile banking security.
- By following these steps, you can significantly reduce the risk of falling victim to mobile banking fraud.

Make this checklist a handy reference and prioritize your mobile banking security!