

Everyday Cybersecurity



Hysun Chung (hysun@hysun.com)
LinkedIn: <https://linkedin.com/in/hysun-c>
X/Twitter: @azmaveth
Blog: <https://azmaveth.com>

Today's Topics

- **Introduction**

- Importance of smartphone privacy and security
- Overview of potential risks

- **Basic Security Measures**

- Strong passwords and PINs
- Biometric security
- Keeping software and apps updated
- Device encryption
- Physical device security

- **Data Privacy**

- Understanding app permissions
- Managing location services
- Controlling ad tracking
- Privacy settings on social media apps
- Safe browsing practices

Importance of Smartphone Privacy and Security

- **Your smartphone: A treasure trove of personal information**
- **Privacy and security: Key to protecting your digital life**



Potential Risks

- **Identity theft**
- **Financial fraud**
- **Data breaches**
- **Unauthorized access to personal information**
- **Location tracking**
- **Malware and viruses**
- **Everyone is a target (Yes, even you!)**

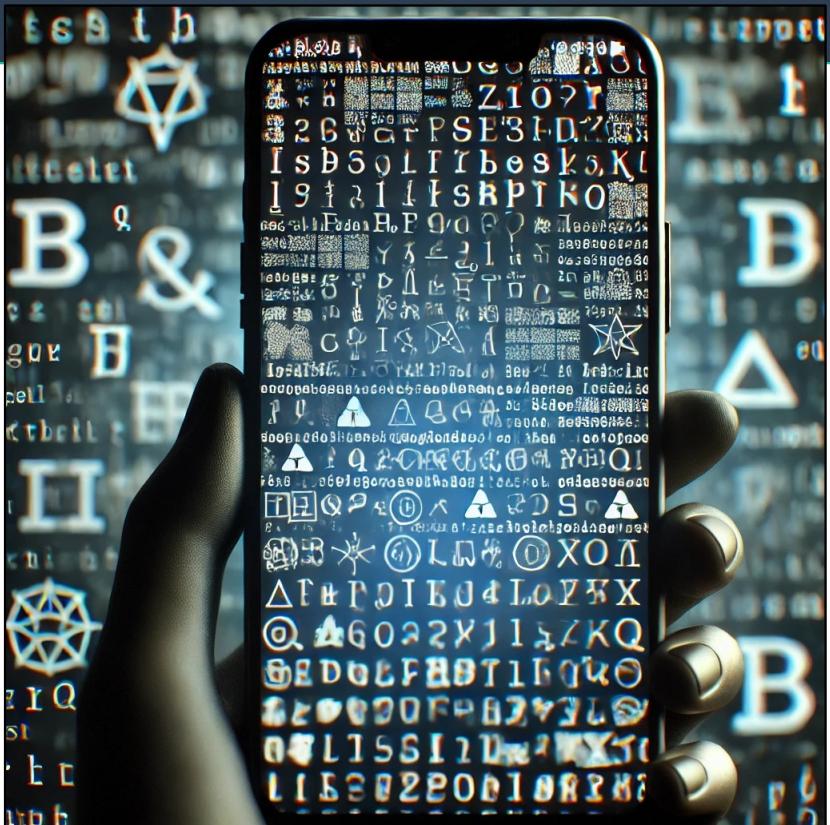
Basic Security Measures

- **Strong passwords and PINs**
- **Biometric security
(fingerprint, face
recognition)**
- **Keeping software and apps
updated**
- **Device encryption**
- **Physical device security**

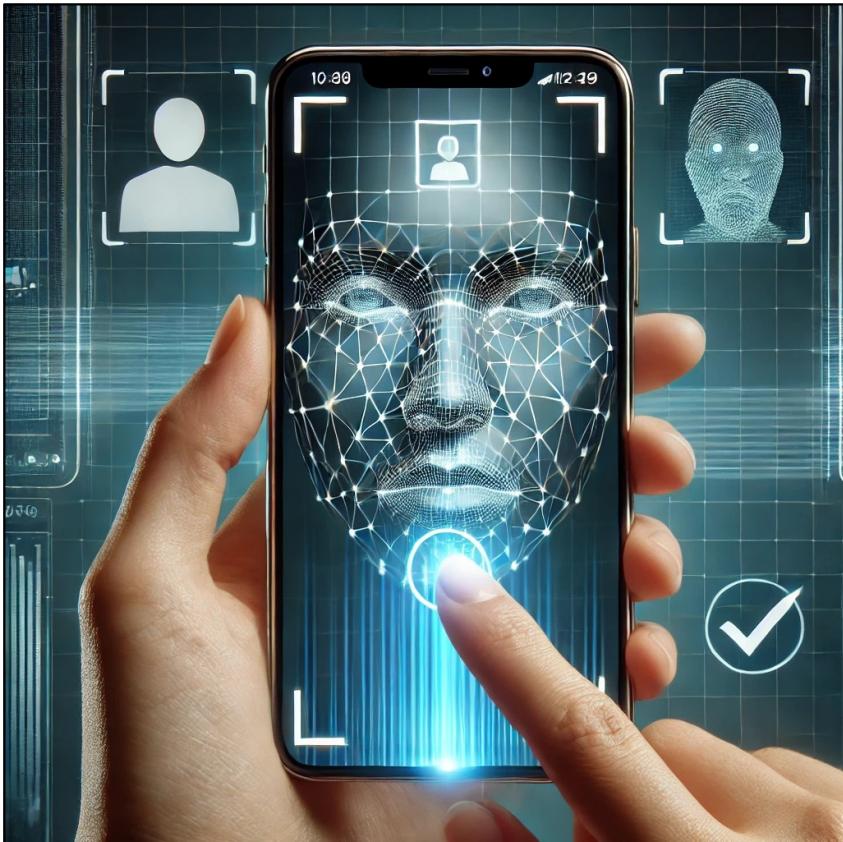


Strong Passwords & PINs

- **Use at least 6 digits for PINs (more is better)**
- **Avoid obvious numbers (birthdays, address, etc.)**
- **For passwords, use a mix of:**
 - Upper and lowercase letters
 - Numbers
 - Special characters
- **Avoid using the same password across multiple accounts**
- **Consider using a password manager**
- **Demonstration: Setting up a strong password**



Biometric Security



- **What is biometric security?**
 - Fingerprint recognition
 - Face recognition
- **Benefits:**
 - Convenient and quick
 - Generally more secure than short PINs
 - Difficult to replicate or guess
- **Considerations:**
 - Not foolproof - can sometimes be tricked
 - May still need a backup PIN or password
- **Demonstration: Setting up fingerprint or face recognition**

Keeping Software and Apps Updated

- **Why updates are important:**
 - Fix security vulnerabilities
 - Improve performance
 - Add new features
- **What to keep updated:**
 - Operating system (iOS/Android)
 - Individual apps
- **How to update:**
 - Enable automatic updates
 - Check for updates manually
- **Demonstration: Checking for and installing updates**



Device Encryption

- **What is device encryption?**
 - Scrambles data to make it unreadable without the key
- **Why is it important?**
 - Protects your data if your phone is lost or stolen
 - Prevents unauthorized access to your information
- **How it works:**
 - Encrypts all data on your device
 - Decrypts data when you unlock your phone
- **Enabling encryption:**
 - Often on by default in newer phones
 - Can be turned on in settings for older devices
- **Demonstration: Checking encryption status and enabling it if necessary**



Physical Device Security

- **Keep your device with you or in a secure location**
- **Be aware of your surroundings when using your phone in public**
- **Don't leave your phone unattended, even briefly**
- **Use "Find My Device" features**
- **Back up your data regularly**
- **Demonstration: Setting up "Find My Device"**



Data Privacy



- **Key topics we'll cover:**

- Understanding app permissions
- Managing location services
- Controlling ad tracking
- Privacy settings on social media apps
- Safe browsing practices

- **Why it matters:**

- Protect your personal information
- Control who sees your data
- Prevent unwanted tracking

Understanding App Permissions

- **What are app permissions?**
 - Requests to access specific features or data on your phone
- **Common types of permissions:**
 - Camera
 - Microphone
 - Location
 - Contacts
 - Storage
- **Why permissions matter:**
 - Control what information apps can access
 - Protect your privacy and security
- **Demonstration: Reviewing and adjusting app permissions**



Managing Location Services

- **What are location services?**
 - Features that use your phone's location
- **Benefits of location services:**
 - Navigation and maps
 - Finding nearby businesses
 - Weather updates
- **Privacy concerns:**
 - Apps tracking your movements
 - Location history being stored
- **How to manage:**
 - Control which apps can access your location
 - Choose when apps can access location (always, while in use, never)
- **Demonstration: Adjusting location settings**



Controlling Ad Tracking



- **What is ad tracking?**
 - Collection of your online activity to show personalized ads
- **How it works:**
 - Apps and websites track your behavior
 - This data is used to create a profile of your interests
- **Privacy concerns:**
 - Extensive data collection about your habits
 - Potential for data breaches or misuse
- **How to limit ad tracking:**
 - Use built-in phone settings
 - Opt out of personalized ads
 - Use privacy-focused browsers and search engines
- **Demonstration: Adjusting ad tracking settings**

Privacy Settings on Social Media Apps

- **Why social media privacy matters:**
 - Control who sees your posts and information
 - Protect personal data from misuse
- **Key privacy settings to review:**
 - Profile visibility
 - Post audience
 - Friend/follower approvals
 - Data sharing with third-party apps
- **Common social media platforms:**
 - Facebook
 - Instagram
 - Twitter
- **Demonstration: Adjusting privacy settings on a popular platform**



Safe Browsing Practices

- **Use secure websites (look for "https" and padlock icon)**
- **Be cautious with public Wi-Fi**
- **Use private browsing mode when appropriate**
- **Clear browsing data regularly**
- **Be wary of phishing attempts**
- **Keep your browser updated**
- **Demonstration:**
 - Identifying secure websites
 - Enabling private browsing
 - Clearing browsing data



Questions?

- **Introduction**
 - Importance of smartphone privacy and security
 - Overview of potential risks
- **Basic Security Measures**
 - Strong passwords and PINs
 - Biometric security
 - Keeping software and apps updated
 - Device encryption
 - Physical device security
- **Data Privacy**
 - Understanding app permissions
 - Managing location services
 - Controlling ad tracking
 - Privacy settings on social media apps
 - Safe browsing practices

Resources

- **Youtube**

- <https://www.youtube.com/@NaomiBrockwellTV>
- <https://www.youtube.com/@AllThingsSecured>

- **Blogs/News**

- <https://www.privacytools.io/guides/category/smartphones>
- NSA's Mobile Device Best Practices

Mobile Device Best Practices from the NSA

National Security Agency | Mobile Device Best Practices

Threats to mobile devices are more prevalent and increasing in scope and complexity. Users of mobile devices desire to take full advantage of the features available on those devices, but many of the features provide convenience and capability but sacrifice security. This best practices guide outlines steps the users can take to better protect personal devices and information.

Airplane mode Bluetooth® Cellular service signal Location Near-field communication (NFC) Recent applications soft key Wi-Fi

BLUETOOTH®
Disable Bluetooth® when you are not using it. Airplane mode does not always disable Bluetooth®.

WI-FI
DO NOT connect to public Wi-Fi networks. Disable Wi-Fi when unneeded. Delete unused Wi-Fi networks.

CONTROL
Maintain physical control of the device. Avoid connecting to unknown removable media.

CASE
Consider using a protective case that covers the microphone to block room audio (hot-miking attack). Cover the camera when not using.

CONVERSATIONS
DO NOT have sensitive conversations in the vicinity of mobile devices not configured to handle secure voice.

PASSWORDS
Use strong lock-screen pins/passwords; a 6-digit PIN is sufficient if the device wipe itself after 10 incorrect password attempts. Set the device to lock automatically after 5 minutes.

APPLICATIONS
Install a minimal number of applications and only ones from official application stores. Be cautious of the personal data entered into applications. Close applications when not using.

SOFTWARE UPDATES
Update the device software and applications as soon as possible.

BIOMETRICS
Consider using Biometrics (e.g., fingerprint, face) authentication for convenience to protect data of minimal sensitivity.

TEXT MESSAGES
DO NOT have sensitive conversations on personal devices, even if you think the content is generic.

ATTACHMENTS/LINKS
DO NOT open unknown email attachments and links. Even legitimate senders can pass on malicious content accidentally or as a result of being compromised or impersonated by a malicious actor.

TRUSTED ACCESSORIES
Only use original charging cords or charging accessories purchased from a trusted manufacturer. DO NOT use public USB charging stations. Never connect personal devices to government computers, whether via physical connection, Wi-Fi, or Bluetooth®.

LOCATION
Disable location services when not needed. DO NOT bring the device with you to sensitive locations.

POWER
Power the device off and on weekly.

MODIFY
DO NOT jailbreak or root the device.

POP-UPS
Unexpected pop-ups like this are usually malicious. If one appears, forcibly close all applications (i.e., iPhone®²; double tap the Home button* or Android®³; click "recent apps" soft key).

*For iPhone X² or later, see: support.apple.com/en-us/HT201330

²Bluetooth® is a registered trademark of Bluetooth SIG, Inc.

³iPhone® and iPhone® applications are a registered trademark of Apple, Inc.

³Android® is a registered trademark of Google LLC.

The information contained in this document was developed in the course of NSA's Cybersecurity mission, including its responsibilities to assist Executive departments and agencies with operations security programs.

UI/OO/155488-20 | PP-20-0622 | Oct 2020 rev 1.1

Mobile Device Best Practices from the NSA



National Security Agency | Mobile Device Best Practices

THREAT/VULNERABILITY	WHAT CAN I DO TO PREVENT/MITIGATE?												
	Update Software & Apps	Only Install Apps from Official Stores	Turn Off Cellular, WiFi, Bluetooth	Do Not Connect to Public Networks	Use Encrypted Voice/Text/Data Apps	Do Not Click Links or Open Attachments	Turn Device Off & On Weekly	Use Mic-Drowning Case, Cover Camera	Avoid Carrying Device/No Sensitive Conversations Around Device	Lock Device with PIN	Maintain Physical Control of Device	Use Trusted Accessories	Turn Off Location Services
Spearphishing (To install Malware)	●	●			●	●							
Malicious Apps	●	●			●								
Zero-Click Exploits	●			●		●							
Malicious Wi-Fi Network/Close Access Network Attack	●		●	●	●	●							
Foreign Lawful Intercept/Untrusted Cellular Network	●	●	●	●	●								
Room Audio/Video Collection	●	●					●	●					
Call/Text/Data Collection Over Network	●		●	●	●	●							
Geolocation of Device	●	●	●	●			●			●			
Close Access Physical Attacks	●						●	●	●	●			
Supply Chain Attacks								●					

Does not prevent (no icon) Sometimes prevents Almost always prevents

Disclaimer of Endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

NSA Cybersecurity

Client Requirements/General Cybersecurity Inquiries: Cybersecurity Requirements Center, 410.854.4200, Cybersecurity_Requests@nsa.gov.
Media Inquiries: Press Desk: 443.634.0721, MediaRelations@nsa.gov.