Signal Security for Democracy Defenders

Part 1: Configure your Phone

Disable Biometric Authentication

Disabling biometric authentication prevents someone from unlocking your device by putting it in your face or forcing your thumb onto the reader.

Android:

1. Navigate to **Settings app.**
2. Navigate to the **Security** or **Biometrics and Security** screen (name can vary).
3. Navigate to **Fingerprint** and Remove or Delete the registered data.
4. Go back to **Security.**
5. Navigate to **Face Unlock** and Remove or Delete the registered data.

iPhone:

1. Navigate to **Settings**
2. Navigate to **Face ID & Passcode**
3. Under "Use Face ID For," deactivate "iPhone Unlock"
4. Optional: deactivate for all other options (e.g., iTunes and App Store)

Disable Voice Commands

Disabling voice commands prevents getting data from your device by speaking to it or forcing you to speak to it.

Android:

1. Navigate to the **Google app.**
2. Tap your **profile picture** in the top-right corner.
3. Navigate to **Settings > Google Assistant > Lock Screen**
4. Disable assistant features on the lock screen.

iPhone:

1. Open the **Settings** app.
2. Scroll down and tap **Siri & Search** (may appear as **Apple Intelligence & Siri** on newer iOS versions).
3. Toggle off **Allow Siri When Locked**.

Hide Notification Content

Hiding notification content prevents someone from seeing the content of your messages while the device is locked.

Android:

1. Open the **Settings app.**
2. Navigate to **Apps & notifications > Notifications > Notifications on Lock Screen.**
3. Disable the **Sensitive Notifications** setting.

iPhone:

1. Open the **Settings** app.
2. Tap **Notifications**.
3. Tap **Show Previews**.
4. Select **When Unlocked** (or **Never** for maximum privacy).

Use a Unique 6-8 Digit PIN

A long and unique password makes it harder to guess or brute-force your PIN to forcibly unlock your device.

Android:

1. Navigate to the **Settings App.**
2. Navigate to the **Security** or **Biometrics and Security** screen (name can vary).
3. Under Device Security, select Screen Lock, then select PIN.
4. Set a new PIN between 6 and 8 digits.

iPhone:

1. Open the **Settings** app.
2. Tap **Face ID & Passcode** (or **Touch ID & Passcode** on older models).
3. Tap **Change Passcode** (or **Turn Passcode On** if not already enabled).
4. Tap **Passcode Options** and select **Custom Numeric Code**.
5. Enter a new PIN of 6-8 digits.

Part 2: Configure Signal (for iPhone and Android)

Change Your Display Name

Using a fake name makes it harder to tie your Signal activity back to you if a group chat or another person's device is compromised.

1. Open the **Signal app.**
2. Tap your **profile picture** on the top-left corner of the screen to access the Settings menu.
3. Tap your **profile picture** again to access your Profile.
4. Tap the top option with your current display name to edit your display name.

Set a Signal PIN

A Signal PIN blocks anybody from transferring your account to another device without that PIN.

1. Open the **Signal app.**
2. Tap your **profile picture** on the top-left corner of the screen to access the Settings menu.
3. Navigate to **Account**.
4. Select Change your PIN, and set a 6-8 digit PIN.
5. Enable Registration Lock.

Optionally, enable PIN reminders to have Signal occasionally ask for your PIN to help you memorize it.

Optimize Signal Privacy Settings

Heighten your privacy on Signal by restricting data sharing and access.

1. Open the **Signal app.**
2. Tap your **profile picture** on the top-left corner of the screen to access the Settings menu.
3. Navigate to **Privacy**.
4. Select **Phone Number,** and set both "Who can see my number" and "Who can find me by number" to Nobody.
5. Under the **Messaging** section, **disable** Read Receipts and Typing Indicators.
6. Under **Disappearing Messages,** set a Default Timer for New Chats of 1 week. This can be overridden for individual conversations if they need to be kept longer or shorter.
7. Under the **App Security** section, set your Screen Lock to 1 minute, **enable** Screen Security and Incognito Keyboard. (Note: Incognito Keyboard and Screen Security are for Android only)
8. Select the **Advanced** menu.
9. **Enable** the Always Relay Calls setting.
    - If you use a VPN with a killswitch enabled, this last step isn't strictly necessary, and you may want to leave it disabled to improve call quality.