OTPhone Documentation

Introduction

OTPhone is a privacy-first communication device built on a locked-down Linux platform. This documentation provides an overview of the device features, security modes, and best practices.

Security Modes

AES Mode (Standard E2EE): End-to-end encrypted messaging with modern authenticated encryption. Best for day-to-day private chat. The server relays ciphertext only, integrity is built in (anti-tamper), and it offers fast performance with low overhead.

OTP Mode (One-Time Pad): Unbreakable encryption when used correctly. Pads must be exchanged in person. Perfect forward secrecy is guaranteed, no computational assumptions required, and it provides the highest confidentiality for sensitive communications.

Key Features

• Locked-down OS: Appliance-like setup that boots straight into OTPhone

• Central relay with optional trust: Server forwards encrypted messages without reading content

• Modes per conversation: Choose AES or OTP per contact

• Pad management: Clear indicators for pad health, offsets, and verification status

• Remote message wipe: Send wipe command online if phone is stolen

• Privacy-first signup: Register with email only

Getting Started

Step 1: Register
Sign up on our website with your email address. No phone number required.

Step 2: Receive device
Your OTPhone will arrive pre-configured and ready to use.

Step 3: Choose a mode
Select AES for everyday E2EE, or OTP for in-person pad exchange.

Step 4: Message
The relay forwards ciphertext while your device encrypts/decrypts locally and manages pad state safely.

Privacy & Security

What the relay sees: The relay only sees minimal routing metadata including sender & recipient IDs, timestamps & message sizes, and encrypted payload blobs.

What stays on your phone: All cryptographic secrets remain on your device including private keys, session state, and OTP/OTP pads & offsets.

Best Practices

- Keep your device updated with the latest firmware
- Use OTP mode for highly sensitive communications
- Exchange pads in person in a secure location
- Never reuse one-time pads
- Enable remote wipe if your device is lost or stolen
- Verify pad checksums after exchange