

Forum: [Hack Forums](#)

Thread: [\[2025\] Anonymous Messaging Toolkit](#)

Dystortion - June 16, 2025, 3:12 pm

Anonymous Messaging Toolkit 2025

Devices • eSIMs • Zero-Log Apps • Hardened Stacks

"If they can subpoena it, design so it doesn't exist."

? Warning ?

- "No-logs" marketing means nothing if architecture still creates logs.
- I listed only projects that are (1) open-source, (2) audited or verifiably peer-reviewed, and (3) have zero known hand-overs as of April 2025 (giving time for newer hand-overs to have occurred).
- Wherever a past legal disclosure happened, I have foot-note exactly what was given so you decide risk.

High Anonymous Messaging AppsSession - Onion-routed, Oxen blockchain, zero metadata. No phone or email ever.

? Audit: Kudelski Security (2024) - confirmed no user logs.

<https://getsession.org>

SimpleX Chat – Serverless; messages hop via disposable relay pairs then auto-wipe.

? Veracrypt Labs audit (Q3 2024).

<https://simplex.chat>

Briar – Works via Bluetooth/Wi-Fi mesh if the internet dies; stores in-app SQLite with forward-secrecy.

? Used in Hong Kong 2024 protests; no seized devices yielded chat history.

<https://briarproject.org>

XMPP over Tor + OMEMO – Pick any self-hosted onion XMPP (e.g. trashserver.net onion).

? "If the server can't see your clearnet IP, it can't log it."

Mail & Alias LayersSimpleLogin (now merged into Proton, but still separate infra) – Create unlimited burner aliases.

? Proton handed over 1 IP in 2021*; SimpleLogin stores only alias <-> target mapping encrypted.

<https://simplelogin.io>

DNMX (dark-net mail relay) – .onion POP3/SMTP gateways with automatic key rotation.

? Zero clearnet surface.

<http://dnmxmailz2xyzabc.onion>

*Proton 2021 case: Swiss warrant forced them to log a single IP retrospectively. No message content was surrendered.

eSIM / SIM Silent.Link – Crypto-only eSIM, UK/EU routing mixed through roaming pools; as of 2025, no disclosures on transparency report.

Nomad "Voucher" eSIMs – Buy Apple/Google gift cards on Paxful -> redeem inside Nomad app ->

zero ID.

Stork Mobile (new 2025) – Accepts Monero, rotates IMSI monthly, API-driven activation via Tor.
CloudSIM Banks – Host SIM cards in a Raspberry Pi abroad; control via VPN. Best for SMS verifications.

Quick-start Burner Flow:

1. Buy Stork Mobile eSIM with XMR.
2. Register Session using that number -> nuke eSIM immediately.
3. Keep Session ID forever; SIM data gone.

Device & OS Hardening (basic) GrapheneOS Pixels – Verified boot, secondary user profiles, network permission toggle per app.

CalyxOS + Orbot “VPN-only profile” – For mid-range Androids.

iOS Lockdown Mode – Not anonymous but decent for receiving messages from less-technical contacts.

USB-C Firewall Adapter (USBGuard-powered) – Blocks hostile chargers / USB implants.

Zero-Leak Settings Checklist:

1. Disable Wi-Fi scanning & Bluetooth scanning.
2. Remove all Google/Apple analytics via network blocklist.
3. Use NetGuard or RethinkDNS to route only chosen apps through Tor/Orbot.

Network CloaksProxifier Chains – Windows/macOS: route selected apps -> SOCKS (Tor) -> HTTPS CDN -> VPN.

dnscrypt-proxy + Tor DNS – Prevents local resolver leaks.

uTLS Padding – Mimic Chrome/Edge JA3/ALPN so TLS fingerprint = normal user.

Meek / Snowflake Bridges – Latest pluggable transports for DPI-nazi countries (China/Iran 2025).

What's your Stack?Found a smaller eSIM broker that takes XMR?

Know a zero-knowledge mail relay I didn't mention?

"Metadata kills. Remove it, or it removes you."

lincoln - July 11, 2025, 6:07 am

very detailed. thahnks

cl0udzz - June 10, 2026, 2:54 am

If anyone wants it <https://monerica.com/> lists lots of sites that accept XMR or are focused on it, to receive sms I always use <https://crypton.sh/> and I've personally never had any problem with them.

Pr0m3th3us - June 12, 2026, 12:33 am

Good list, i have a couple TUTs on IRC over TOR and IRC over I2p.