

NYX Secure Communication Phone

Military-Grade Privacy. Zero Trace. Total Control.

Why NYX?

NYX is not just a phone. It's a hardened, surveillance-proof communication device engineered for users who demand absolute privacy, untraceable communication, and zero digital footprint. Built on a custom GrapheneOS Pixel architecture, NYX offers a full-stack solution for military, executive, journalistic, and privacy-focused individuals who cannot afford compromise.

1. Hardware Security

- Hardened Pixel Device: Secure, verified hardware with support for advanced privacy OS.
- Verified Boot: Ensures firmware integrity at every startup.
- No Google Components: Eliminates telemetry, tracking, and forced syncing.

2. Hardened Operating System

- GrapheneOS: Industry-leading secure mobile OS with full app sandboxing.
- No Root Access: Prevents any unauthorized low-level modifications.
- App Isolation: No app can access another's data or permissions.
- Internet Restrictions: Only NYX app and NYX VPN routing are granted internet access.

3. IMEI: Not a Threat

- NYX does NOT use a SIM card. Without cellular connection, IMEI is never transmitted.
- IMEI is only broadcast on mobile networks (via SIM). With Wi-Fi-only operation, it's inert.
- MAC address randomization ensures even Wi-Fi networks can't track the device identity.

4. Network & Communication Anonymity

- NYX Communication Protocol: Secure, decentralized, end-to-end encrypted messaging.
- No Metadata: NYX leaves no trace of IP, user IDs, contacts, or time stamps.
- All traffic exits through the NYX network using obfuscated bridges, bypassing censorship

and traffic analysis.

- All network activity is automatically anonymized before reaching the internet.

5. Forensic Resistance

- No Logs: NYX doesn't store messages, contacts, or keys.
- Auto-Delete Options: Messages can self-destruct after being read.
- No Accounts: No phone number, username, or ID is required to use NYX.
- No Cloud: No data is ever synced or backed up to third-party servers.

6. Physical Security

- Strong Password Encryption: All data is protected with GrapheneOS's hardware-based full disk encryption.
- Auto Lockdown: Device locks immediately after use or can be wiped manually.
- Optional Faraday Pouch Use: Complete RF shielding for ultimate stealth.

7. Real-World Anonymity Practices

- Use over Wi-Fi only – never insert a SIM.
- Tether via burner devices or public networks.
- Disable GPS, Bluetooth, and unnecessary sensors.
- Use MAC-randomizing settings with every new Wi-Fi connection.

8. Security Summary

Feature	NYX Protection
-----	-----
IMEI/Cellular Tracking	Eliminated (No SIM, No Cellular)
Metadata Surveillance	None (Zero-Log Protocol)
Network Fingerprinting	Hidden ()
App-Level Spying	Prevented (App Sandboxing)
Forensics	Data-Free, No Recovery Possible
Google/Apple Tracking	None (No Play Services Installed)
Account Linking	Not Possible (No Registration)