

DIGITAL SOVEREIGNTY & DEVICE HARDENING TOOLKIT

A Step-by-Step Security Protocol for Survivors of Digital Intrusion & Coercive Control

Prepared By: Low Country Boil Advocacy Network
Project Focus: Domestic Espionage Prevention

Resource Type: Self-Defense & Advocacy Toolkit
Technical Tier: Universal Hardening Protocol

FORENSIC CONTEXT: Technology is a central coordinate in modern coercive control. Unlike traditional hacking, digital domestic espionage rarely relies on sophisticated viruses or external brute-force attacks. Instead, intruders exploit standard, legitimate administrative conveniences—such as multi-device cloud synchronization, active OAuth session persistence (cookie hijacking), shared credentials, accessibility overlays, and automated virtual routing. This toolkit provides survivors and advocates with a systematic, non-technical protocol to sever backdoor bridges, invalidate active session tokens, and reclaim absolute physical and digital sovereignty over their devices and identities.

1. CRITICAL CLOUD ACCOUNT & IDENTITY HARDENING

- [] **Force Global Session Invalidation:** Navigate to your primary cloud account security dashboards (Google, Apple, Microsoft) and select 'Sign out of all other sessions.' This immediately revokes any active, cached session cookies and OAuth authentication tokens that an intruder may have cloned from your browser to mirror your account without a password.
- [] **Disable Auto-Fill & Credential Synchronization:** Access your account synchronization settings and toggle off credential, draft, and password sync. This severs the shared cloud pipeline, preventing an intruder's keystrokes, personal typing dictionary, pre-saved predictive phrases, or clipboard history from syncing directly into your phone's keyboard memory.
- [] **Purge Lookalike Recovery Channels:** Audit all associated security recovery profiles. Inspect your recovery settings to identify and expunge lookalike recovery email addresses or unauthorized backup numbers, replacing them exclusively with clean, private channels that are secured under your sole physical control.
- [] **Decommission Multi-Factor VoIP Backdoors:** Verify that your multi-factor authentication (MFA) numbers do not route to virtual VoIP lines (like Google Voice, TextNow, or Burner accounts) controlled by an intruder. Lock your verification codes strictly to your trusted mobile hardware carrier, or switch to app-based authenticators.
- [] **Enroll in Advanced Protection Services:** For high-risk environments, enroll your primary accounts in Google's Advanced Protection Program or Apple's Lockdown Mode. These settings block unauthorized recovery-bypass attempts, restrict non-secure API scripts, and require physical USB security keys (such as YubiKeys) for all authentication requests.

2. MOBILE DEVICE & HARDWARE SANITIZATION

- [] **De-Authorize Cloud & Ecosystem Backups:** On your mobile device, navigate to 'Accounts and Backup' (Android) or 'iCloud' (iOS) and fully disable background ecosystem synchronization. This severs the local-to-cloud pipeline that treats your personal physical phone as a shared database workspace, which can silently push unauthorized background settings onto your screen.
- [] **Wipe Keyboard Cache & Predictor History:** Navigate to your keyboard settings (Samsung Keyboard, Gboard, or iOS Keyboard) and select 'Clear personalized predictions' and 'Reset keyboard settings.' This permanently wipes pre-saved text fragments, draft clipboards, and predictive phrase patterns from your device's interface memory.
- [] **Audit Accessibility Services & Device Admin:** Go to Settings > Accessibility > Installed Apps and Settings > Security > Device Admin Apps. Search for and immediately revoke permissions for any unrecognized applications, custom shortcuts, launcher overlays, or automation scripts (such as accessibility wrappers or hidden mirroring tools) used to bypass standard system boundaries.
- [] **Perform a Cryptographically Secure Factory Reset:** If you suspect deep-level system modification or persistent spyware, execute a complete factory reset. Ensure your device is fully wiped and set up as a brand-new device—do not restore from a shared cloud backup that could re-inject cloned security tokens or mirrored script registries.

3. THIRD-PARTY & CONNECTED PLATFORM DECOUPLING

- [] **Sever Connected App Integrations:** Log into major social platforms (Facebook, Instagram, Snapchat, TikTok) and navigate to 'Apps and Websites' or 'Authorized Integrations.' Revoke access to any third-party app connections. This stops background data transfer bridges that can silently route private attachments and logs directly to shared storage lockers.
- [] **Invalidate Cross-Platform Session Cookies:** Manually sign out of all active social and professional apps across every browser, tablet, and PC, then sign back in. This forces platform servers to regenerate fresh cryptographic authentication tokens, immediately destroying any active 'pass-the-cookie' remote control loops.
- [] **Decommission and Blacklist Staging Contacts:** Completely delete any recognized virtual numbers, burner lines, or staging contacts from your physical device's contact directory. Because social and communication apps automatically crawl and sync device contacts, keeping staging lines in your directory can automatically suggest secure communication bridges back to the intruder's profiles.
- [] **Terminate Active Chat & Bot Sessions:** Open your primary communication apps (Telegram, Discord, Signal, WhatsApp) and navigate to 'Settings > Devices' or 'Active Sessions.' Select 'Terminate all other sessions.' Audit all bot permissions, revoking any unauthorized API connectors or automation channels used to scrape, translate, or redirect chat data off-grid.

RECLAIMING AUTONOMY & CONTROL

Reclaiming your digital sovereignty is not just about technology—it is about boundaries, safety, and agency. Intruders rely on complexity to enforce confusion, but when you strip away the technical smoke and mirrors, you expose their shadow infrastructure. By systematically invalidating sessions, severing sync bridges, and isolating recovery details, you transform your technical awareness into real physical protection. You have the facts. You have the receipts. You have taken back control of your life.