WHAT TO DO WHEN SHTF DIGITALLY

Emergency Protocol for Privacy Breaches, Device Seizures, or Digital Compromise

Print this. Store offline. Memorize key parts.

Print it. Keep a copy offline in your go bag or hidden stash. Run through it like a fire drill before you ever need it. In crisis, don't improvise. Follow the steps. Lock down fast, communicate clean, wipe what you must, and rebuild from safe ground. Stay calm. Move quiet.

LOCK DOWN IMMEDIATELY

- **Change all critical passwords** (start with email, crypto, financials)
- **Revoke access** to devices and sessions (check Proton, Signal, Nextcloud, etc.)
- **Enable 2FA** if not already on (use hardware token or app, *not SMS*)
- **Cut internet access** to compromised device (airplane mode + kill WiFi)
- **Encrypt devices** if not already done (LUKS, BitLocker, VeraCrypt)

CONTACT TRUSTED ALLIES

- Use **Signal** or **Session** (not SMS, not Telegram)
- If compromised, switch to backup burner comms
- Stick to **code words** and **pre-agreed fallback phrases**
- Never disclose full details unless fully secure and verified

BURN PATHS + WIPE DATA

- **Wipe browser history + cookies** (especially if fingerprinted identities were active)
- **Use secure deletion tools**:
  - Linux: `shred`, `wipe`, `srm`
  - Windows: Eraser, BleachBit
- **Factory reset** mobile devices from recovery mode
- **Securely erase drives** with DBAN or physical destruction
- **Nuke cloud backups** (Proton Drive, Dropbox, iCloud) if compromised

RESET FROM CLEAN GROUND

- Set up **new device or Live OS** (Tails or freshly wiped Linux)
- Generate **new logins, keys, and burner accounts**
- Rebuild access **with compartmentalization** (separate identities, apps, browsers)
- Assume old aliases or emails are compromised

REMEMBER

If you're unsure it's safe, **don't touch it.**
No rash logins. No panicked messages.
Silence buys you time.

STAY QUIET. STAY SHARP. STAY FREE.