🧠High-Tier OPSEC Tips

> *"They can't find you if you were never there."*

This file is your upgrade. These tips go beyond the basics and are designed for users operating in high-risk, high-anonymity environments like the dark web.

🌛Micro Persona Split

One alias = one purpose. Never mix buying, messaging, forum posting, or uploading. - Don't use the same name/email/PFP across sites. - Use different slang, typos, or grammar per alias.

💟MAC Layer Ghosting

- Use `macchanger` or `randommac` to spoof your MAC every boot.
- Combine with hardware serial number masking (advanced).
- Never connect to darknet from your regular router — use public WiFi + Tails.

👐🏼Network Cloaking Stack

Use layered routes: - Public WiFi → VPN1 → Tor (Bridge) → VPN2 (inside VM) → .onion - Bonus: Add SSH tunnel or proxychains

---

🖤Stylometry Disruption

- Use slang/grammar different from your real life.
- Use random punctuation, lowercase-only, emoji overflow, or AI-based writing changers.
- Tools: Anonymouth, Torghost stylometry disruptor (if updated)

😉Metadata Nuking

- Use `mat2`, `exiftool`, or `scrub` to destroy image/document metadata
- Don't trust just "removing GPS" — thumbnails, camera serials, and even fonts leak
- Always upload screenshots taken inside Tails or VMs, not your host OS

😬Burn Protocol

If you feel you're being traced: - Burn the identity (delete all accounts & devices) - Factory reset routers, shred logs, overwrite drives (dban, shred, etc.) - Never reuse anything again

---

👎🏿Miscellaneous High-Risk Ops Tips

- Never save passwords, use KeePassXC inside an encrypted volume
- Never use real timezone, language, or keyboard layout
- Use voice changer or avoid voice completely if contacting vendors
- Avoid Telegram, WhatsApp, and anything linked to SIM or clearnet

---

> "Privacy isn't a setting. It's a strategy."