DIGITAL DISAPPEAR STARTER GUIDE

How to Reduce Your Digital Footprint FAST

1. BURN YOUR OLD IDENTITY

Why it matters:
Your existing accounts and digital habits bleed data. They link you to surveillance, spam, profiling, and exploitation. Cut ties now.

ACCOUNT DEATHLIST

- Delete or anonymize old accounts (start with Google, Facebook, Instagram, Twitter, LinkedIn)
- Use [https://justdelete.me] to find deletion links fast
- For accounts you can't delete, strip personal information and change email/password
- Obfuscate recovery info (burner emails, throwaway phones)

EMAIL AND USERNAMES

- Stop using real name emails.
- Ditch your long time handles (yes, even gamer tags and socials)
- Set up encrypted burner email (ProtonMail, Tutanota)

SOCIAL SCRUB

- Unfriend everyone you wouldn’t trust with your home address if you are using your real identity
- Delete old posts, photos, and likes
- Turn off location history

2. EXIT THE DATA MONOPOLIES

Big Tech is your biggest surveillance vector. They track what you search, where you go, who you talk to, what you say, and when you sleep.

DUMP GOOGLE

- Use Startpage or DuckDuckGo for search
- Install GrapheneOS or CalyxOS on your Android, or switch to a de-Googled ROM
- Use F-Droid and Aurora Store instead of Google Play

LEAVE META

- Delete Instagram and Facebook
- Stop using WhatsApp. Switch to Signal or Session
- Remove Meta Pixels from your browser (use uBlock Origin, Privacy Badger)

MICROSOFT AND APPLE

- Windows: disable telemetry, or switch to Linux
- iOS: block ad tracking, or move to a hardened Android alt

3. BUILD YOUR BURNER INFRASTRUCTURE

Set up your parallel digital life. This is your alt identity stack.
Use it for: logins, signups, messaging, payments.

EMAIL

- ProtonMail or Tutanota
- AnonAddy or SimpleLogin for burner aliases

PHONE NUMBERS

- MySudo, JMP.chat, or Silent Link for pseudonymous numbers
- NEVER reuse numbers linked to real identity

PAYMENTS

- Use Monero or Cash
- Buy gift cards with cash or crypto
- Use privacy respecting stores like Privacy.com for masked cards

FILE STORAGE

- Cryptomator + Google Drive
- Encrypt Individual files before cloud (picocrypt)
- Proton Drive
- Self host with Nextcloud

4. MASK YOUR SIGNAL

If you're using the same browser, DNS, and IP as before, you're trackable no matter what. Fix it.

DNS AND NETWORK

- Use NextDNS or ControlD (customized, encrypted DNS)
- Set up your router to use DNS-over-HTTPS (DoH)
- Kill smart devices leaking data

BROWSER

- Use Firefox (hardened) or Brave
- Install: uBlock Origin, Privacy Badger, HTTPS Everywhere, NoScript
- Use containers to split personas (Firefox Multi-Account Containers)

MOBILE

- Install NetGuard or TrackerControl (on Android)
- Remove Google Play Services or use sandboxed version (via MicroG)

5. SCRUB YOUR DEVICES

Don't disappear online if your phone or laptop keeps giving you away.

WIPE YOUR DEVICES

- Do a factory reset + overwrite free space
- Reinstall OS from verified ISO (Pop OS, Debian, Qubes)
- Encrypt disks (LUKS, VeraCrypt, BitLocker)

FRESH START

- On phones: install CalyxOS, GrapheneOS, or LineageOS
- On laptops: use Linux, ideally Qubes for compartmentalization

FINAL TOUCH

- Destroy or securely wipe old hard drives (use shred or DBAN)
- Log out of all old cloud accounts and delete backups
- Start using a Live OS for high-risk tasks *(see Lesson 10 in UNTRACEABLE)*

WANT TO GO DEEPER?

This is just your starter pistol. The full race is in *UNTRACEABLE: Handbook for the Digital Dissident*.

Inside the book:

- Full threat modeling breakdowns
- DIY encrypted comms setup
- Burner phone workflows
- Local first cloud alternatives
- Advanced device hardening
- Live OS and hidden volumes

https://untraceabledigitaldissident.com/