Digital Fortress Cheat Sheet: Secure Your Computer

1. USE A PRIVACY OS

- Qubes OS (compartmentalized)

- Tails OS (USB, leaves no trace)

- Linux (Debian, Ubuntu, Pop!_OS)

- AVOID macOS, Windows, Chrome OS

2. BLOCK MUSK / THIEL TOOLS

- Uninstall Twitter, Tesla, Starlink, Palantir

- Disable voice assistants: Cortana, Siri, Google Assistant

- Use LOCAL accounts only

3. FIREWALL + VPN

- Use Pi-hole or Portmaster to block surveillance

- VPNs: Mullvad, ProtonVPN (no logs, not US based)

4. SECURE BROWSING

- Use Firefox or Brave

- Extensions: uBlock Origin, Privacy Badger, NoScript

- Use Tor for anonymity

5. ENCRYPT EVERYTHING

- Full disk: LUKS (Linux), VeraCrypt (Windows)

- File encryption: Cryptomator, GPG

6. ANTI-SPY TOOLS

- Use webcam and mic covers

- Turn off Bluetooth and Wi-Fi when not in use

- Secure deletion: BleachBit, MAT2

7. BEHAVIOR MATTERS

- Avoid Google, Facebook, X, WhatsApp

- Do not click unknown links or use strange USBs

- Use private messengers like Session, Briar

EXTRA TOOLS

- Remove metadata with MAT2

- Anonymous email: ProtonMail

- Private DNS: NextDNS, DNSCrypt

NEVER trust default settings. Use open-source. Stay aware.