Hitchhiker’s Guide

A summary and action guide

Michael Obernhumer

29.4.2025

1 Actionable Guide for online Anonymity

1.1 Introduction

This is a summarized checklist and to-do list aimed at increasing privacy and anonymity on the internet. It has been compiled based on the official Hitchhiker's Guide to Online Anonymity not including the links in the guide. Please note that this guide is **neither exhaustive nor guaranteed to be foolproof**. Its purpose is to provide a quick overview and actionable steps, **not** to replace the in-depth explanations and context found in the original guide. For comprehensive details, background information, and reasoning behind each recommendation, please refer to the full Hitchhiker's Guide. Keep in mind that none of these methods are foolproof, and each comes with potential trade-offs and risks.

1.2 Index

- Actionable Guide for online Anonymity
  - Introduction
  - Index
  - Your Network
    - Your IP address
    - Your DNS and IP Requests
    - Your RFID enabled devices
    - The Wi-Fi and Bluetooth devices around you
    - Rogue Wi-Fi Access Points
    - Traffic Anonymization
    - Some Devices can be tracked even when offline
  - Your Hardware Identifiers
    - Your IMEI and IMSI
    - Your Wi-Fi or Ethernet MAC address¶
    - Your Bluetooth MAC Address
  - Your CPU
  - OS and App Telemetry services
  - Your Smart Devices
  - Yourself
    - Your Metadata
    - Your Digital Footprint
    - IRL and OSINT
    - Your Face, Voice, Biometrics and Pictures
    - Gait Recognition and Other Long-Range Biometrics

    * Phishing and Social Engineering
  - Malware, exploits, and viruses
    * Malware in your files/documents/e-mails
    * Malware and Exploits in your apps and services
    * Malicious USB Devices
    * Malware and backdoors in your Hardware Firmware and Operating System
    * Your files, documents, pictures, and videos
    * Watermarking
      · Pictures, Video and Audio¶
      · Printer Watermarking
    * Pixelized or Blurred Information
  - Your Crypto Transactions
  - Your Cloud Backup and Sync Services
  - Microarchitectural Side-channel Deanonymization Attacks
  - Local Data Leaks and Forensics
  - Bad Cryptography
  - No-Log Policies
  - Some Advanced targeted techniques
  - Some bonus resources
  - General Preparations
    * Picking your route
  - Steps for all routes
    * Getting used to using better passwords
    * Getting an Anonymous Phone Number
      · Burner Phone
      · Anonymous Prepaid SIM
      · Online Phone Numbers (Riskier)
    * Get a USB key

1.3 Your Network

1.3.1 Your IP address

Your IP address is easily accessible and can reveal identifying information about you. To protect your privacy, it's important to conceal or obfuscate your origin IP address — the one that can be linked directly to your identity. This can be achieved using one or a combination of the following methods:

- **Public Wi-Fi networks** (free)

- **The Tor anonymity network** (free)
- **VPN services used anonymously** (e.g., paid with cash or Monero)

1.3.2 Your DNS and IP Requests

By default, your DNS requests are handled by your Internet Service Provider (ISP), which logs them.

These requests are typically sent in plaintext, making them easy to intercept and monitor.

Recent studies have shown that **DNS over Tor** offers the most effective DNS privacy among available options. However, even this method can potentially be compromised through other techniques.

To further enhance your privacy and anonymity, consider the following approaches:

- **Tor Hidden DNS Services** or
- **ODoH (Oblivious DNS over HTTPS53)** — This method helps prevent a single intermediary from correlating the DNS query with your IP address. However, it is not effective against a **Global Passive Adversary (GPA)** who can monitor multiple parts of the communication chain simultaneously.
- **DoHoT (DNS over HTTPS over Tor)** — A newer method that routes encrypted DNS over the Tor network, offering enhanced anonymity. This approach requires some Linux expertise.

Other DNS privacy practices include:

- Using a **private DNS resolver** (e.g., Pi-hole, NextDNS, or DNS over Tor)
- Enabling **DoH (DNS over HTTPS)** or **DoT (DNS over TLS)**
- Using browsers that support **ECH (Encrypted Client Hello)** — currently, only Firefox-based browsers support ECH, and it must be enabled manually
- Ensuring your browser supports **OCSP (Online Certificate Status Protocol)** — this is enabled by default in most modern Firefox and Chromium-based browsers

It's also important to note that simple IP requests (e.g., loading a webpage) can still leak information about the site you're visiting, as many websites use unique IP addresses.

To address these concerns as thoroughly as possible, this guide will later recommend two primary solutions:

1. **Using Tor**
2. **Implementing a virtualized, multi-layered setup**, such as **VPN over Tor** (e.g., DNS over VPN over Tor or DNS over Tor)

1.3.3 Your RFID enabled devices

RFID in everyday items (cards, passport, phone, etc.) can be scanned without your knowledge, posing privacy risks like tracking or de-anonymization.

1. **Only carry RFID items when needed.**
2. **Use RFID-blocking wallets or pouches.**
3. **Be cautious in stores—some may scan all RFID tags.**
4. **Shield devices during sensitive activities (e.g. Farrady cage).**

1.3.4 The Wi-Fi and Bluetooth devices around you

Wi-Fi and Bluetooth signals are used to track your location and movements, even without GPS. Devices constantly scan nearby signals and send this data to companies like Google and Apple. This can be used for precise tracking—even through walls—by analyzing signal interference.

1. **Avoid carrying identifiable devices during sensitive activities.**
2. **For high privacy, stay in areas shielded like a Faraday cage.**
3. You could also try turning of Wi-F, Bluetooth, GPS,… but you cannot really trust these settings

1.3.5 Rogue Wi-Fi Access Points

Rogue Wi-Fi access points (APs) can trick your device into connecting to fake networks using de-auth attacks and spoofed portals. Once connected, attackers can monitor your traffic, steal credentials, and even bypass VPNs/Tor with advanced techniques.

1. **Avoid connecting to unknown/public Wi-Fi networks.**
2. **Always use a VPN/Tor (or VPN + Tor) on public networks.**
3. **Verify captive portals carefully, don't enter credentials unless you're sure it's legit.**

1.3.6 Traffic Anonymization

Tor and VPNs help protect your privacy, **but they're not invincible**. Advanced attacks like **correlation** and **timing analysis** can de-anonymize you by matching encrypted traffic patterns to known destinations or users — even **without decrypting anything**.

Common Attacks:

- **Fingerprinting**: Match your encrypted Tor traffic to website patterns.
- **Timing Attacks**: Correlate when you connect to Tor/VPN with when someone accesses a site.
- **Counting Attacks**: Match download/upload sizes across networks.

Mitigations:

- Don't access local services through anonymizers (e.g., don't Tor into your own university network).
- Avoid heavily monitored networks (e.g., corporate or government).
- Use **VPN over Tor** (or **Tor over VPN**) to add layers and confuse correlation attempts.
- Use **public or residential Wi-Fi** for added unlinkability.

Important Notes:

- Global surveillance adversaries (e.g., NSA) can still break anonymity with enough data.
- Tor usage **alone** might flag you as suspicious in some contexts.
- Tools like behavioral analysis or Wi-Fi/Bluetooth tracking can still deanonymize you indirectly.

For more, check out:

- Attacks on Tor GitHub
- Tor research survey
- Tor 0day post

> Bottom line: Tor helps, but **don't rely on it alone** — especially against well-funded adversaries.

1.3.7 Some Devices can be tracked even when offline

Modern devices like:

- iPhones (iOS 13+)
- Samsung phones (Android 10+)
- MacBooks (macOS 10.15+)

can still broadcast Bluetooth signals even when turned off. Nearby online devices can pick this up, making offline tracking possible.

TL;DR: Don't bring these devices during sensitive activities or put them in a Faraday pouch. "Off" doesn't mean invisible.

1.4 Your Hardware Identifiers

1.4.1 Your IMEI and IMSI

Every phone has two unique IDs:

- **IMEI** (device ID – tied to the hardware)
- **IMSI** (SIM ID – tied to your phone number and provider)

Whenever you connect to a mobile network, **both are logged** by operators and often shared with app makers, OS providers, and governments.

Why it matters:

- Even **anonymous SIMs** can betray you if reused on a phone with a known IMEI.
- **Antenna logs** can match your "burner" to your real phone based on signal strength and time.
- **IMEI sale records** can trace the phone back to you—even if bought with cash, e.g. CCTV, Antenna logs.
- **IMSI** is often tied to your ID (when SIMs require registration).
- **Apple/Google** can track historical usage of your IMEI/IMSI.
- **IMSI-catchers** (like Stingrays) can fake antennas to intercept calls, messages, or impersonate your number.

Best practices:

- Use **burner phones** and **cash-bought SIMs** not tied to your identity.
- Avoid reusing phones or SIMs.
- Consider **anonymous online SIM services** that accept crypto (like Monero).

Note: Some "privacy" phones (e.g., Purism Librem) **still don't support IMEI randomization**, so full anonymity is tricky.

TL;DR: IMEI + IMSI = uniquely trackable. Use a truly separate device + SIM for sensitive actions.

1.4.2 Your Wi-Fi or Ethernet MAC address¶

Every device with Wi-Fi or Ethernet has a **MAC address** — a unique ID for your network hardware.

Why it's a privacy risk:

- It can be **linked to the buyer** via manufacturer records (serial number + MAC).
- Even cash-bought laptops may be traceable through **CCTV and antenna logs**.
- OS vendors like **Apple, Google, Microsoft** log MACs for services like "Find My Device."
- **Routers log MACs**, and many ISP-provided routers can be remotely accessed.

- **Public/commercial networks** may track nearby MAC addresses (e.g., for traffic analysis).

Key point: If you used a device normally before using it for sensitive activity, it's likely already linked to you.

Protect yourself:

- **Randomize your MAC address** — supported on Android, iOS, Linux, Windows 10/11.
- **macOS does not support MAC randomization** — not ideal for privacy.
- Avoid using your personal device for sensitive activities.

TL;DR: MAC addresses can silently link you to a device and place. Use MAC randomization or separate hardware.

1.4.3 Your Bluetooth MAC Address

Your **Bluetooth MAC** is another unique identifier — like your Wi-Fi MAC, but for Bluetooth.

Why it matters:

- Manufacturers & OS vendors **log Bluetooth MACs**, potentially linking them to your identity or purchase.
- Logs + billing info + **CCTV footage** + **antenna data** can be used to trace it back to you.

Privacy risks:

- Can be used to **track your presence** in stores, public places, etc.
- Some **vulnerabilities** still exist, even with protections.

What to do:

- **Disable Bluetooth** entirely in BIOS/UEFI if possible — or via your OS if not.
- On **Windows 10**, toggle the Bluetooth device in *Device Manager* to force address randomization.

TL;DR: Bluetooth tracking is less risky than Wi-Fi MAC tracking but still a concern. Disable it if not needed.

1.5 Your CPU

Modern **Intel** and **AMD CPUs** include hidden subsystems:

- **Intel Management Engine (IME)**
- **AMD Platform Security Processor (PSP)**

These can **run even when your PC is "off"**, have **network access**, and have had **serious vulnerabilities** in the past. Many consider IME a **backdoor**.

Privacy Tips:

- Prefer **AMD CPUs** — fewer issues and no known remote backdoors.
- **Disable IME/PSP** in BIOS (if possible).
- Consider using **Coreboot/Libreboot** (if supported).
- Use **virtual machines** for sensitive tasks.
- Only use on **anonymous public networks**.

Check for vulnerabilities:

- **Linux**: `spectre-meltdown-checker`
- **Windows**: InSpectre

1.6 OS and App Telemetry services

Most modern OSes — **Windows, macOS, Android, iOS, Ubuntu, Apps** — **collect telemetry by default**, even if you opt out. This data can include:

- Device identifiers
- App usage
- Location info
- Network activity
- Hardware/software details
- …

This data **can identify and track you**, even if anonymized.

What to Do:

- Use **privacy-focused OSes** (e.g., Linux distros like Qubes).
- Block telemetry via firewalls, host files, or tools (e.g., **O&O ShutUp10++** for Windows).
- Minimize app installs; prefer **FOSS alternatives**.
- Avoid smartphones for sensitive activity.

1.7 Your Smart Devices

Smartphones and smart devices constantly track:

- **Location, audio, habits, nearby devices**
- **Photos, accounts, networks**
- Data is often sent/stored **unencrypted**, even if you opt out.

Other culprits: smartwatches, speakers, fitness trackers, cars, tags.

Leave all smart devices behind for sensitive activities.

1.8 Yourself

1.8.1 Your Metadata

Metadata = info **about** your activity, not the content.
Think: *who* you contacted, *when*, *where* — not *what* was said.

Example:
You call an oncologist, then family — no one hears the call, but **the pattern speaks volumes**.

Metadata often includes:

- Your **location** (from phones, OS, apps, websites)
- **Time and duration** of activity
- **Devices** involved
- Your **contacts** and their frequency

This data is:

- Used in **geofencing warrants** (authorities request all devices at a place/time)
- **Sold** to militaries and third parties
- **Correlated** across ISPs, VPNs, platforms (even if each holds only part of the picture)

Even with a VPN:

- The **VPN sees your traffic**, but not your ID

- The **ISP sees your ID**, but not your traffic
  Together? They **could** trace you.

Minimize metadata leakage.
Use privacy tools + stay aware of what your devices reveal — even *without* your input.

1.8.2 Your Digital Footprint

Your **digital footprint** is more than just what you post or search — it's **how** you behave online. And that behavior is *shockingly unique*.

Behavior = Identity Even if you mask your IP, use a VPN, or disable cookies, systems can still identify you through:

- **Stylometry**: The way you write (word choice, grammar, punctuation, etc.)
- **Behavioral biometrics**: Typing speed, rhythm, mouse movements
- **Browser fingerprinting**: Fonts, extensions, screen size, OS, hardware
- **Keystroke logging**: Even if you don't submit a form
- **Cursor tracking & click behavior**: Your subconscious habits are identifiers

Even things like: > "You always click the same button first"
> "You use specific words or typos often"
…can be used to **link your identity** across platforms.

How to Minimize Fingerprinting:

Tech helps, but behavior matters most.

1. **Use privacy-focused tools**:
   - Tor Browser (with JS disabled if needed)
   - Firefox with privacy extensions (like uBlock Origin, NoScript, CanvasBlocker)
   - Anti-fingerprinting OSes (like Tails or Qubes OS)
2. **Act differently with anonymous identities**:
   - Change typing habits (speed, spelling style)
   - Use different phrasing or vocabulary
   - Vary mouse/click behavior
   - Don't use your usual site/app flow or bookmarks

> You're playing a role. Don't leave behavioral breadcrumbs.

1.8.3 IRL and OSINT

Even with good privacy tools, sharing real-life details over time can expose you. This is where **OSINT (Open-Source Intelligence)** comes in—collecting public data like forum posts, photos, metadata, and social media to link identities.

Example: Hacker Jeremy Hammond was caught after casually mentioning personal facts online. Over time, those added up.

OSINT Resources:

- OSINT Framework
- Awesome OSINT GitHub
- ReconTool

Stay Safe:

- Don't reuse stories, habits, or writing styles
- Avoid specific dates, places, or job info
- Act like a completely different person online

You should never share real individual experiences/details using your anonymous identities that could later lead to finding your real identity.

> Every post is a puzzle piece. Don't let them add up.

1.8.4 Your Face, Voice, Biometrics and Pictures

Even if you're super careful, **your body can betray you**—especially your face.

Face Recognition Is Everywhere:

- Platforms like **Facebook, Google, Snapchat** use it to tag and organize photos.
- Even **random selfies in public** can capture your face and link you to a location and timestamp.
- Uploaded images often include metadata (EXIF), and even without it, AI can estimate **when and where** the photo was taken.

Want to See This in Action?

- Bellingcat's guides & videos show how **facial recognition** and **geolocation** are used in real investigations:
  - Facial Recognition in Investigations
  - Reverse Image Search Guide
  - Sun & Shadow Geolocation

Bottom Line:

- **Avoid selfies** and **public appearances** if anonymity is critical.
- Don't share photos or recordings tied to your voice, face, or body.
- Remember, once your image is online, it's **almost impossible to take back**.

1.8.5 Gait Recognition and Other Long-Range Biometrics

Even if your **face is covered**, you're still not safe from modern surveillance.

Gait Recognition:

- Cameras can ID you just by **how you move**—not just your steps, but how your **muscles shift**.
- **Changing your walk doesn't work**—they see through that.
- Best defense: **loose clothing** that hides muscle movements.

Other Biometrics:

- **Earlobes**, **skull shape**, **eye behavior**, **lip movements**, and even **emotion analysis** from posture/face.
- Facial coverings like balaclavas may **draw more attention** and still reveal enough to ID you.

Mitigation Tips These only reduce risk—they don't guarantee protection:

- **Mask** – can defeat some face recognition.
- **Baseball cap** – blocks top-down CCTV.
- **Sunglasses** – hide eyes (try Reflectacles).
- Try 3D-printed **face/gait spoofers** like FG-01.

But remember: **trying too hard to hide** can make you more suspicious and lead to **human review**.

TL;DR: Modern surveillance can identify you by **how you move, talk, look, and behave**. Tools exist to reduce exposure, but none guarantee invisibility—only mitigation.

1.8.6 Phishing and Social Engineering

Phishing tricks you into revealing info by impersonating trusted sources—via fake emails, texts, or calls. It's often used to steal credentials or install malware.

Defense:

- **Stay skeptical** of unexpected messages.
- **Don't click suspicious links** or download unknown files.
- **Verify** requests through official channels.
- Use **2FA** when possible.

1.9 Malware, exploits, and viruses

1.9.1 Malware in your files/documents/e-mails

Malware can hide in common files (PDFs, images, videos, Office docs) using tricks like steganography or exploits in outdated software. Even tiny images in emails can leak your IP or trigger malicious downloads.

Defense:

- Avoid opening files from unknown sources.
- Keep your software up to date.
- Use **virtual machines** or **sandboxes** when handling risky files.

1.9.2 Malware and Exploits in your apps and services

Even privacy tools like Tor or Brave can have hidden exploits unknown to the developers but known to attackers.

How to Protect Yourself:

- **Never fully trust any app.**
- **Always use the latest version** and verify downloads with checksums/signatures.
- **Use virtual machines** to isolate risky apps and browsers.

1.9.3 Malicious USB Devices

Cheap, widely available devices like "BadUSBs" can be used to silently hack your system just by being plugged in.

They can:

- Deploy malware
- Log your keystrokes
- Track your location
- Take control of your device

These can be hidden in cables, mice, keyboards, or USB sticks.

How to Protect Yourself:

- **Never plug unknown USB devices** into sensitive machines.
- **Use data-blocking adapters** for charging-only connections.
- **Disable USB ports in BIOS** if you don't need them.
- **Avoid using public charging stations** without blockers.

Even skilled users can't detect advanced USB-based malware without forensic tools.

1.9.4 Malware and backdoors in your Hardware Firmware and Operating System

Malware can exist not just in apps—but deep within your **hardware, firmware**, and **operating system**.

Real-World Examples:

- **Intel IME**: A manufacturer-embedded backdoor allowing remote access.
- **Interdiction**: Attackers insert malware *before* hardware reaches you (e.g., in transit).
- **Rootkits**: Stealthy malware that runs deeper than the regular operating system.

Mitigation (though limited):

- Protect physical access to your hardware
- Reflash firmware or BIOS from a trusted source if possible
- Use devices that allow disabling manufacturer backdoors (e.g., Coreboot-supported hardware)

Once malware is in firmware or hardware, **detection and removal become extremely difficult**—especially if it's by the manufacturer itself.

1.9.5 Your files, documents, pictures, and videos

Most files—especially **images and videos**—contain hidden metadata that can reveal sensitive details.

What kind of data?

- **EXIF** in images: GPS location, camera model, time/date
- **Videos**: Can include GPS data, recording device info

- **Documents**: Author name, edit history, software used

Why it matters: Even if metadata doesn't name you, it can show **where and when** you were somewhere—info that can be cross-referenced with other sources like CCTV or online posts.

Mitigation:

- **Strip metadata** before uploading (using tools like `exiftool`, `mat2`, or built-in settings)
- **Always** double-check all files—even plain text—for hidden data

Be meticulous. Leaked metadata has unmasked identities before—don't let it happen to you.

1.9.6 Watermarking

1.9.6.1 Pictures, Video and Audio¶

Even if there are **no visible watermarks**, files from commercial platforms may include **invisible watermarks** to track or identify you.

- Zoom can embed **video** and **audio watermarks**.
- Apps like Adobe Premiere can insert tracking via extensions.
- Watermarks often survive **compression** and **re-encoding**.
- Devices used to film (e.g., lenses or microphones) can be **fingerprinted**.

Bottom line: Avoid using known commercial tools or double-check their watermarking options if you're handling sensitive content.

1.9.6.2 Printer Watermarking

Yes, **your printer might betray you**, even offline.

- Many printers print **invisible dots** that identify the model and possibly the print time.
- This is called **printer steganography**

Mitigation tips:

- Print in **black and white only** (color often triggers watermarking).
- Use the EFF's list of printers **without tracking dots**:
  EFF printer list

Always assume your media might be watermarked unless you've verified otherwise.

1.9.7 Pixelized or Blurred Information

Blurring or pixelating sensitive data **is not secure**. Adversaries can often **recover** the original information.

Why blurring/pixelizing fails:

- Tools like **Depix** GitHub can **reverse blurred or pixelated text**, especially if a known font or structure is used.
- Deblurring/pixel recovery is common in **OSINT** (Open Source Intelligence).
- Even **photo enhancement** tools (like MyHeritage's Photo Enhancer) can be enough to **reveal or infer details**.
- Videos aren't safe either — recovery techniques can also work on **video frames** Video de-pixelation blog

Best practice:

> **Do not blur. Do not pixelate. Always use solid black redactions.**

That means: crop or overlay black boxes permanently. Never rely on cosmetic effects to hide info — it's not enough.

1.10 Your Crypto Transactions

The Myth: "Crypto = Anonymous":

Wrong. Most cryptocurrencies like **Bitcoin** and **Ethereum** are **pseudonymous** — not anonymous.

Every transaction is:

- **Publicly visible** on a blockchain.
- **Permanently recorded**.
- **Linkable** via patterns, reused addresses, exchange logs, IP traces, etc.

Where deanonymization happens:

- **Creating a wallet** via Tor or VPN → stays anonymous.
- **Converting fiat** (EUR/USD) to crypto → not anonymous due to **KYC** laws at exchanges (Coinbase, Kraken, Binance, etc).
- **Cashing out crypto** to a bank → easily traced.
- **Using mixers/tumblers** → risky and often ineffective due to:
  - Centralized logs
  - Demixing possibilities
  - Legal gray areas (money laundering risks)

Better Option: Monero (XMR):

- **Privacy by design**:
  - Ring signatures
  - Stealth addresses

  - Confidential transactions

- Still not *perfect* — but the best available for privacy-conscious users.

1.11 Your Cloud Backup and Sync Services

Many cloud services like iCloud, Google Drive, OneDrive, and Dropbox claim to use encryption, but they still hold the keys to your data, meaning they can access it if needed. They also scan and index your files for analytics or legal reasons.

What You Can Do:

1. Encrypt your data before uploading.
2. Use zero-knowledge services like Tresorit or Proton Drive.
3. **Avoid cloud backups for sensitive data.**

1.12 Microarchitectural Side-channel Deanonymization Attacks

A recently published attack can link your anonymous identity to a known alias, like a public Twitter handle, breaking anonymity—even with good OPSEC.

How It Works The attack uses invisible iframes and font fingerprinting to detect what fonts are installed on your system. These patterns are unique enough to track users across sessions and link multiple identities together. Even privacy features like "Do Not Track" won't stop it.

Mitigation:

- **Use NoScript Browser Extension** (recommended): Blocks scripts and prevents these attacks.
- **Tor Browser** already blocks the attack by default (via NoScript 11.4.8+).

Important Notes:

- Closing all activity tied to your public identity before using an anonymous one is essential.
- Using separate browsers or VMs alone does not prevent this attack.

1.13 Local Data Leaks and Forensics

Law enforcement can extract data from phones and laptops—even if encrypted. This can happen during investigations or random checks like border crossings.

Smartphones Tools like GrayKey and Cellebrite let police unlock and analyze devices.
Read more:

- UpTurn: Mass Extraction
- NYT: Police Can Break Into Your Phone
- Vice: iPhones Can Be Unlocked

Forensic Tools:

- EnCase Guide (PDF)
- FTK Toolkit
- SANS DFIR Videos

OS Security:

- Johns Hopkins: Mobile Security Overview

Laptops Use full disk encryption, virtualization, and compartmentalization to reduce risk.

1.14 Bad Cryptography

"Don't roll your own crypto" is a common warning for good reason—crypto is hard to get right. Strong cryptography takes years of research, is open source, peer-reviewed, and tested in the real world.

Avoid apps or services that:

- Use custom or closed-source crypto
- Modify existing algorithms
- Use terms like "military-grade encryption" without transparency

Use:

- **Hashes**: SHA-3, BLAKE2 (ok: SHA-256/512; avoid: SHA-1, MD5)
- **Disk encryption**: AES-256 with HMAC-SHA-2/3, ChaCha20, Serpent, TwoFish
- **Password storage**: Argon2 (i/id), scrypt (ok: bcrypt; last resort: PBKDF2; avoid: SHA, MD5)
- **HTTPS**: TLS 1.3 (or TLS 1.2)
- **Signing**: ed25519/ECDSA + ECDH (ok: RSA 4096; avoid: RSA 2048)
- **SSH**: ED25519 or RSA 4096

1.15 No-Log Policies

Many VPN and email providers claim to have "no-log" policies, but they're still legal entities and can be compelled to start logging by court orders—often without your knowledge.

Key takeaways:

- Providers can be forced to log data, regardless of their policies.
- You won't be notified if you're being monitored.
- Warrant canaries exist but remain unproven in court.

Mitigation:

- Use VPNs that accept **cash or Monero**.
- Always **use VPNs over Tor** to hide your identity from the provider.
- Don't rely solely on provider claims—assume they can be compromised.

Trust no one. Design your privacy stack under the assumption that "no-log" might just mean "not yet logging."

1.16 Some Advanced targeted techniques

Read the resources linked on the official guide!

Even if you have great digital hygiene, **high-skilled adversaries** can still breach your defenses—especially if they know where your devices are. These attacks often involve **physical access, hidden malware, or exploiting side channels** (like sound, light, vibrations).

Examples of Advanced Attacks:

With Malware:

- **Router Infection:** Send data out via a compromised router.
- **Light/Camera Attacks:** Watch light variations from keyboards or displays to extract data.
- **Sound-Based Attacks:** Use fan noise, HDD noise, or ultrasonic sounds to transmit information.
- **Electromagnetic Attacks:** Leak data via screen emissions, HDD vibrations, or power lines.
- **Acoustic/IR Attacks:** Use hacked cameras to communicate with malware via infrared light.
- **RAM Wi-Fi Hack:** Turn RAM into a covert Wi-Fi transmitter (!).

Without Malware:

- **Wall Imaging:** Use tiny wall vibrations to map people's positions.
- **Snack Bag Reflections:** Use reflections on shiny surfaces to reconstruct a room.
- **Floor Vibrations:** Track people and emotions through footsteps.
- **Light Bulb Spying:** "Hear" conversations by observing vibrating light bulbs.

Realistic Threat Level:
Most individuals aren't targeted like this.
However, **nation-states**, **corporate espionage**, or **high-value targets** can be.

Mitigations:

- Use devices only on **trusted power sources**.
- Keep devices away from **cameras** and **microphones**.
- Use **soundproofed rooms** and **Faraday cages**.
- Avoid talking near **visible light bulbs** or **reflective surfaces**.
- **Buy hardware offline** from random stores.
- **Limit physical access** to your machines.

1.17 Some bonus resources

Read the resources linked on the official guide!

Bonus Resources for Deeper Learning:

- Whonix Data Collection Techniques
- ToS;DR: Terms of Service, Didn't Read
- EFF Privacy Advocacy
- List of Surveillance Projects (Wikipedia)
- Gwern's Death Note Anonymity Essay
- Michael Bazzell's OSINT Techniques Book
- Freehaven Anonymity Bibliography

Transparency Reports (How often companies hand over user data):

- Google
- Facebook
- Apple
- Cloudflare
- Discord
- GitHub
- … and many more.

Bottom line:
If your adversary is skilled enough and determined enough, no setup is 100% safe.
Stay paranoid, stay careful, but don't go crazy unless you have to.

1.18 General Preparations

Personally, in the context of this guide, it is also interesting to have a look at your security model. And in this context,we only have one to recommend:

Zero-Trust Security ("Never trust, always verify").

Here are some various resources about what Zero-Trust Security is:

- DEFCON, Zero Trust a Vision for Securing Cloud
- From the NSA themselves, Embracing a Zero Trust Security Model

1.18.1 Picking your route

This guide will only go down the Qubes OS route as this is probably the most secure. If you need something immediately have a look at the Tails route.

Note that the Qubes route will afford several investments such as a dedicated laptop.

1.19 Steps for all routes

1.19.1 Getting used to using better passwords

Passphrases > Passwords:

Passphrases (like `purple-fish-drum-sky`) are more secure and easier to remember than complex passwords (`Tr0ub4dor`&3).

Tips for Strong Passphrases:

- Use **4+ random words** (more = better).
- Avoid **quotes**, **personal info**, and **common words** only.
- Make it **easy to remember and type**.
- **Don't reuse** across accounts.

Use KeePassXC to store long, unique passwords for every service locally.

Try useapassphrase.com for examples and entropy.

1.19.2 Getting an Anonymous Phone Number

Skip this if you don't need to register anonymously on platforms that require phone numbers.

1.19.2.1 Burner Phone

- **Buy a basic phone** (ideally a dumbphone with removable battery) **with cash** at a flea market/shop **without CCTV**.
- **Leave your real phone on at home** to avoid metadata leaks.
  - If possible, leave your phone doing something (for example, watching YouTube on autoplay) to obscure the metadata trail further.

- **Never turn the burner on at home or near your real phone**.
- Disable Bluetooth, never connect to Wi-Fi, and test the phone elsewhere.
- Power the phone off, remove the battery (if possible) and put it in a farrady bag when not in use.

1.19.2.2 Anonymous Prepaid SIM

- Harder to get due to ID laws (check SIM registration wiki).
- **Buy with cash** and **no ID**, avoid cameras.
- Recommended: **GiffGaff (UK)** — no ID, lets you change number twice.
- **Power off the burner** after activation/top-up and before returning home.

1.19.2.3 Online Phone Numbers (Riskier)

- Only use after securing your anonymous setup.
- Best paid options (accept Monero, no ID):
  - crypton.sh
  - virtualsim.net
- Riskier/free options (use at your own risk):
  - https://oksms.org
  - https://sms24.me
- It is more convenient, cheaper, and less risky to just get a pre-paid SIM card from one of the physical places that still sell them for cash without ID.

> Avoid shady marketplaces and never use your real identity.

1.19.3 Get a USB key

Skip this step if you have no intention of creating anonymous accounts on most mainstream platforms, but you will want anonymous browsing; or if the platforms which you will use allow registration without a phone number.

Get at least one or two decent size generic USB keys (at least 16GB but we would recommend 32GB). Please do not buy or use gimmicky self-encrypting devices. Some might be very efficient but many are gimmicky gadgets that offer no real protection