Hitchhiker’s Guide

A summary and action guide

Michael Obernhumer

23.4.2025

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.

2 Index

3 Your Network

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)

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)

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).**

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

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.**

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**.

3.6.1 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.

3.6.2 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.

3.6.3 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.