**Using Internet Cafés**

**Isolating internet usage from ID**

* **Alter physical location from where you access the internet**
  + This is called your internet uplink and ‘going off-site’
  + Cafes, airport, hotspot, any anonymous network
* **Using an uplink that is connected to you is an anonymity risk, a high one at that**

**Internet Café**

First, follow the OPSEC rules

Use busy Cafes in busy locations – less noticeable

Use where staff have a low technical capabilities

Change the cafes you use with no pattern

Don’t use local cafes

* Vary distance away from where you live so you don’t create a pattern based on the cafes you use

Vary times you use them

Don’t use the same one twice

* If you do, do not sit in the same spot

Don’t take a phone with you that you don’t want to associate an ID with

Avoid CCTV

Where a disguise and look normal, blend in

Avoid talking to people without standing out unneccisasarily

Sit where you can see people coming, up against a wall

* So you can power off device if necessary

Superglue fingertips to avoid fingerprints

Don’t leave DNA – take drinks, waste, food, cigarettes back with you

Don’t use cafes own devices as everything can be logged and monitored

* Completely vulnerable if you are on a machine someone else owns
* If a message must be sent on the machine, make sure its encrypted before on another machine
* Pre-encrypt message on home machine, move to USB, then take USB to café and send
* Don’t send directly to contacts to avoid providing meta-data, upload to a public forum

Don’t login to anything that is associated or will deanonymise

* Nothing that you have logged into from your real IP either

Can use live OS on café machine

* Almost as good as using your own device

Portable apps on a USB

Use encrypted tunnels where possible

Everything you type could be logged including usr and pwd

**Public Wi-Fi Hotspots**

Follow OPSEC rules

Access hotspots from a distance

* The right equipment can reach up to 12km etc.

Use a VM to access network

* Virtual isolation

VPN/Firewall hardware router

* Physical isolation

Must still use anonymising, privacy and security measures as you can still be deanonymised via the cafes IP etc. (location, time etc.)

The network can log everything you do

* To where
* The content if no encryption
* MAC addr
* MITM (no encryption)
* Traffic injection (no encryption)

If risks are high enough, use open-source hardware

* Raspberry Pi

MAC changers

* Hotspot will log MAC of network adapter on machine
* Use different disposable network dongles (per alias)
  + As well as changing the MAC of it
  + Don’t carry more than one at same time especially if associated with different IDs
  + Use different dongle for each ID
* Disable wifi cards or any other wifi tech not being used

If you’re using Tor, use a bridge or pluggable transports

* Or use SSH or VPN as first hop as that’ll look less suspicious
* Make sure no association to you from first hop
* Make sure no data leaks before you set up your encrypted tunnel
  + Disable services not being used
  + Firewall to not send traffic without VPN or SSH
  + Need a special firewall rule set for public hotspots really

Use portable router and connect to network via that

* Physical isolation
* Change MAC
* Different Wi-Fi dongle
* Separate router per alias

Never use MacOS or Windows as they can leak

* Use QubesOS or Whonix with a network VM

Place a privacy screen so people can’t see your screen unless directly looking at it

Don’t ever visit the location of hotspot if you want to be anonymous

Change pattern of hotspots

Avoid hotspots near to you

Vary distance of hotspots you use

Don’t use same one twice

* Same MAC ties you as same user
* Should be changing MACs anyway

Different times of using hotspots

Avoid CCTV

Sit in Starbucks to connect to hotspot across the road

Connect for as short a time as possible

* As little data as possible
* Disconnect every hour, then change MAC and reconnect
* This helps preventing geolocation

Connect in heavily populated area

Keep moving if possible

* Change location periodically

Sit where you can see people, back towards wall

Wiggle.net is a website that shows available hotspots in your area

* Wardriving.com/code.php

Wi-Fi pineapple router

Mini smart router with OpenWRT

* Can even flash Pineapple onto it

AcrylicWifi

Cain and able

Wi-Fi LAN monitor

WirelessNetView

NetSpot

* Mac

**Kismet**

* Linux/debian