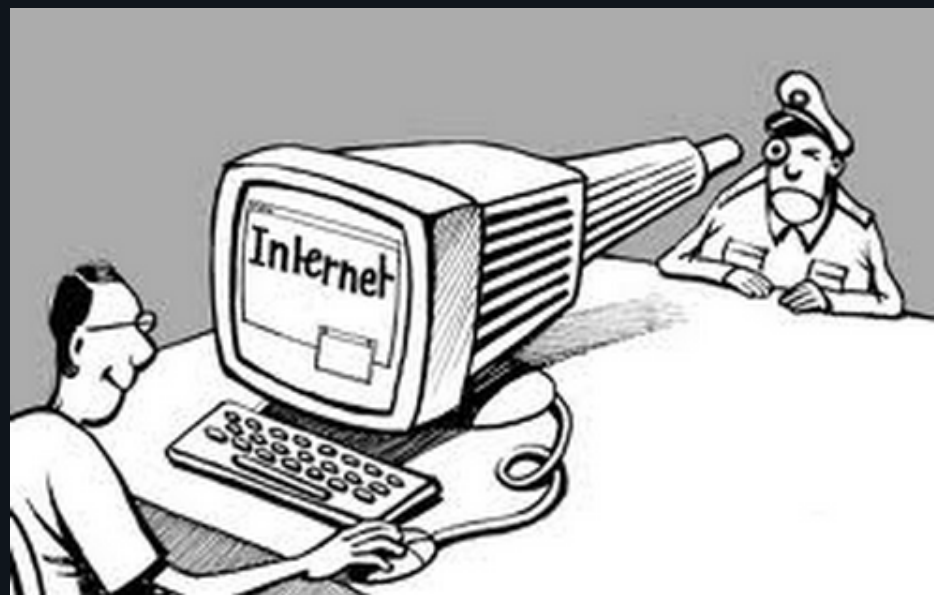




HOW TO BE INVISIBLE ONLINE

and other security

CONTENTS

1. INTRO

2. WEB BROWSING

3. PROXY SERVERS & VPN



5. EMAIL

5. YOUR SMARTPHONE IS A COP

6. SECURITY CULTURE

7 CONCLUSION

INTRO

Capitalism seeks to attach value to everything and everyone, our daily activity in the world and online is no different. From the websites you visit, the shops you buy from and even the times at which you do these things, it is all logged and analyzed so value can be extracted from you more effectively. The other side to this surveillance makes it possible for the state to police us at all times. By now many of you will have learned of a Philadelphia protester who was photographed setting a police car ablaze in the George Floyd rebellion, and was subsequently identified by the FBI by analyzing protest footage, social media posts and online shopping records. We leave a trail in the course of our everyday lives, and we present this guide to better online anonymity in hopes it will prevent similar occurrences in the future.

We only know what we know so we're sharing that. There are more knowledgeable comrades out there, and other resources available which we encourage y'all to seek out.

The road to liberation will be a struggle and we will need everyone with us. Let's cover our tracks on the way there. ♥

Web browsing

It is correct to assume all your online activity is being monitored and stored. Just about everything online is setup to identify you, your interests, your social circle and even the device you're using. It's no secret Google is always spying. We recommend not EVER using them (chrome browser & Google search engine) nor Safari or Edge, but if you must you can at least do this:

- **Surf in incognito/private mode**
 - **This will prevent passwords and browsing history from being logged by a Google but does not stop other trackers from following you across websites & logging other details like your IP address & Network provider.**
- **Third party browser extensions/Adblockers**
 - **There are a few extensions you can add to your browser to keep third parties from following you across websites. The Electronic Frontier Foundation EFF offers one such extension called Privacy Badger: <https://privacybadger.org>**
 - **Works with Chrome, Opera and Edge Browser**
 - **Also with Android version of Firefox**

Web browsing continued

There are many alternatives out there, so if you don't want Google and the State watching everything you do try these tools:

- **Browsers**

- **Tor**

- **Stops trackers**
 - **Anyone spying can only see you're using Tor but can't see what you're up to.**
 - **Makes all Tor users look the same to prevent identification**
 - **Triple encrypts your online traffic (encryption makes stuff unreadable to an outsider)**



- **Other browsers: Brave, DuckDuckGo, Opera**

- **Search Engine: DuckDuckGo**

- **Collaboration Tools**

- **Instead of using Google docs, use Riseup Pads: pad.riseup.net**
 - **Cryptpad.fr gives client side encryption and offers a few collaboration tools**

Proxy Servers & VPNs

Other tools for evading online surveillance & restrictions are proxy servers and VPNs

- **Proxies**

- Online gateways to the internet that help hide your IP address and can allow you to get around content restrictions
- There are many free proxy servers online, a quick search will get you one
 - Proxy use can sometimes cause performance issues (i.e. streaming or downloading certain content)

- **VPN**

- Encrypts your traffic by creating tunnel to the VPN server
- Hides activity from your ISP (internet service provider i.e. Comcast or AT&T)
- Some browsers have a VPN integrated (i.e. Opera), you can also download a free one
 - (i.e. Proton VPN [android, windows, macOS, iOS, GNU/Linux])

EMAIL

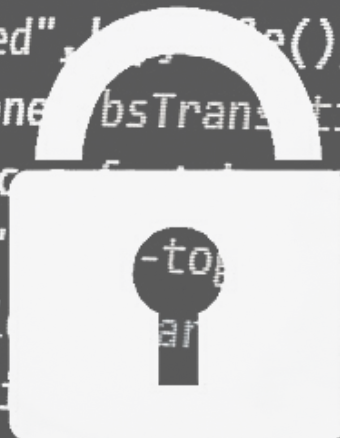
Secure your email communications by using encryption. Every email you send passes through multiple servers and is perfectly readable by third parties when not protected. Encryption encodes your communication so that only you and the recipient can read it.

- **Protonmail**

- **Protonmail is free and encrypts messages end-to-end between protonmail users**
 - **When communicating with non-protonmail users, you can use PGP (pretty good privacy) or Encryption for outside recipients. Protonmail has the steps for either of these methods on its site.**

- **Other encrypted email services**

- **Tutanota, Librem Mail, TorGuard private email**



YOUR PHONE IS A COP

Everything we've shared to this point applies to those activities on your phone as well. What distinguishes our phones from a home computer is it makes our movement in the world traceable. Every cell tower and wireless router you come into contact with can and will log your phone. Law enforcement too has the ability to mimic a cell tower with a device called a Stingray. This machine can capture device characteristics, intercept communications and even deny you service. Next time you go to the protest, leave your cell phone at home or at least leave it in airplane mode if you intend to get into some shit.

Most of us rely on our smartphones heavily throughout our day: they are useful like that. However, as one comrade put it "all technology is military technology" so we should be diligent and assume there is always some back door into our lives through this tech.

- **Voice, Video & Messaging**
 - **Signal. That's it. Download and use Signal. It's end-to-end encrypted.**
- **Metadata**
 - **When we snap a photo on our smart phone it is encoded with data that tells about the device that captured it and even the time and place. If you post photos online, you should remove this data first.**
 - **There are many ways to do this and apps that can do it for you so look up steps for whatever type of phone you're using.**

Security Culture

Treat your technology like an eavesdropping stranger. If you wouldn't discuss it in front of a stranger, don't talk about it online, on your phone, or better yet, at all. How we show up in the fight to abolish the current world isn't for clout or or social media likes anyway.

In some cases private or crucial information must be communicated by technological means, which is why we've presented what we have, but always remember there are risks and this should only ever occur between trusted individuals. Talk to your homies and your family members to create a culture of awareness, so everyone knows their rights if the feds or the pigs knock on someone's door.

When you go to the protest, what are you wearing that might be traceable back to you? Are your tattoos showing? What alias will you use so people aren't shouting your name for all to hear? If you have your phone on you, did you turn off the fingerprint and facial recognition access features so police can't use them to get in if you're apprehended?

Protecting ourselves is also protecting our loved ones and comrades.

Conclusion

Government agencies and law enforcement have the resources to comb the internet for information about us, and spy on us. Private corporations also want to know everything about us, and in the course of the struggles to come will partner with the State to suppress anything that threatens their profitability & power.

We must take every precaution to protect ourselves and others from State repression, which means whatever plans we make or actions we take sometimes won't be things we can ever talk about to anyone. If you declare the State your enemy, take it seriously because they certainly will.

This guide is by no means a guarantee of protection against surveillance, but can at least prevent capitalist powers from having a full picture of what we're doing. The internet is a tool for us to share and interact, let's do everything we can to mitigate the harm it can cause to our people.

Long live Anarchy!

