Cole’s 2025 OPSEC Guide V1.1

Updated 9/9/25

FOREWORD

Operational security (or OPSEC) is about making sure information can’t be used against you. There is a lot of information about you online, and if you’ve used the internet for long enough, you’ve probably interacted with chronically online nerds who use Sherlock (or similar skid tools) to try and find information about you online. I know, because I used to be good at doxxing people myself (something I regret now) and this guide is how I covered my ass.

USERNAMES

I NEVER use the same username site to site anymore. Tools like Sherlock make it insanely easy to jump from website to website and figure out who you are. I always keep my usernames short and ambiguous. I always use common item names, such as starburst, pepper, coke, or sprite, and if I need a unique username, I used Bitwarden to generate it for me. I’ve seen people get doxxed just because their handle was tied back to a Chess.com account with their full name on it. One simple mistake and you are fucked.

OPERATING SYSTEMS

Operating systems DO play a role in OPSEC, but not as much as people like to claim. It’s good to run something secure like Linux or GrapheneOS (I personally use both) if you’re worried about being watched, but the real enemies are other people, not glowies. Just make sure you are running a relatively new version of MacOS/Windows/Linux and you should be good. Nobody can remotely install software anymore (unless there is a zero day in the software you are using)… We are not in the 90s. Now, if you ARE being watched by the feds, I would install anything FOSS as possible. But if you’re reading this on my website… You probably aren’t, lmao.

IDENTIFIABLE INFORMATION

DO NOT SHARE ANYTHING IDENTIFIABLE ONLINE. I cannot stress this enough. This means no last name, no first name (I know this is hard), nothing about the country/state you are living in, **NOTHING**. Anything can and will be used against you by other people. I have doxxed people in the past from simple mentions of their state, bordering cities, and other minor information. People typically do not think twice about this stuff, but it is crucial

in keeping your OPSEC pristine. Same goes for mail. If you use the Dark Web, a lot of vendors recommend using your first and last name for "items" you might get. I strongly advise against this. I have always used a cartoon characters name for my mail, so it is ambiguous for who it is meant for. I have never had any mail be seized and/or searched (I don't buy off of DWMs anyways, I am 1000% sober) and probably never will due to the name on the package being "Batman" lol. I use Google's "Results about you" as well as heavily worded messages/phone calls to Whitepages-like websites to get my shit off of them. Most of them have easy ways of getting this information removed, and it might take you an hour to get everything related to you off of search engines. It always comes back, though, so try and be meticulous about it.

POLICE/LAW ENFORCEMENT

You can probably assume my perspective on law enforcement due to the way I talk about "feds" and "glowies" lol. The best way I deal with police is simple: If I am suspected of a crime, **I DON'T TALK. I ASK FOR A LAWYER AND SHUT UP.** My grandfather was a detective, and the easiest cases to solve were the ones where people ran their mouths. Never consent to searches, never chat with detectives, and don't try to explain yourself. Nobody in law enforcement is your friend. A good example of what to do is what Nick Fuentes did when he was being questioned, and Don't Talk to the Police by James Duane. You are required to talk to them during a traffic stop or a potential DUI, but other than that, shut up and ask for a lawyer. **This should be common sense**.

EVERYTHING ELSE

If you're going to do dumb shit online, separate it from your real life. I keep a burner laptop with TailsOS on it, and if I need to use it, I'll go somewhere public where I'm not on camera. Never mix your main device with risky activity. Keep everything encrypted and secure. Make sure you have a long password generated by Bitwarden on every website as well (this is very important). And most importantly, maintain your OPSEC. VPNs are fine for basic privacy, but if you want real anonymity, Tor is the way to go. It's slower, but it makes tracking you back to your real identity a lot harder, especially when combined with a burner device. Social media is another weak spot. Never follow people you know in real life, and never interact with accounts that have your school, city, or job in their bio. Also make sure you know your threat model. If your problem is just trolls or doxxers, you don't need CIA-level paranoia. If you're worried about law enforcement, you have to treat every move like it is evidence. OPSEC only works if you know what you're defending against.

First draft of my 2025 OPSEC guide. Not fully finished yet, but the main points are covered.