Operational Security on the Internet

The internet has become central to daily life, but most people use it without thinking about how much information they give away. Operational security, or opsec, is the practice of controlling what you expose and how you protect your devices. It is not a switch you flip on or off, it is an ongoing process that depends on your goals and your awareness. Perfect privacy does not exist. Every action online creates data that is recorded by companies, governments, and sometimes criminals. The purpose of opsec is not to disappear but to reduce unnecessary exposure and make attacks against you harder to carry out.

Use a VPN

Every time you connect to a website, your request passes through your internet service provider. They see your IP address, your system details, and the time of each request. That information is logged and often kept for years. A virtual private network encrypts the traffic so outsiders cannot read it and replaces your IP address with one from the VPN server. Good options for beginners are ProtonVPN and Mullvad. Both are affordable and simple to set up. Always enable the kill switch so your computer never leaks your real IP if the VPN drops. Think of it as putting on a mask before entering a crowded place. You cannot control the crowd but you can control how you appear to them.

Strengthen Your Passwords

Weak passwords are still the easiest way to lose accounts. Attackers use tools that can test millions of guesses in seconds. The best defense is to use a password manager that creates long unique phrases for every account. KeePassXC is free, open source, and works offline. Use combinations of unrelated words, symbols, and misspellings. Example: bottle river stone1 shadow!train roof. Long and strange phrases are harder to break and easier to remember than random single words. Store your master password safely on paper or a flash drive so you are never locked out. The goal is to remove single points of failure.

Limit Public Information

Open source intelligence means finding details about you from information that is already public. The danger is that most leaks come from things you shared yourself. A photo of your street, your school name in a profile, or even a casual username can be enough for someone to connect the dots. Avoid posting your full name, address, or identifiable backgrounds in pictures. Do not recycle the same email address or handle across different platforms. Every small clue can add up. Reducing your footprint online is as important as any software setting.

Safer Browsing

Most browsers track your behavior by default. A better option is to use privacy focused browsers that block trackers and resist fingerprinting. Brave is a simple option for beginners

while Librewolf is stricter but removes convenience features. Add uBlock Origin to stop ads and malicious scripts. Safer browsing does not mean no browsing, it means reducing what companies can collect about you.

Choose Secure Hardware

The computer you use is part of your security. Old ThinkPads are recommended because they are cheap, durable, and built with hardware switches for the camera, microphone, and network. They can be bought second hand for little money and are more than enough for everyday use. A solid machine is the foundation of good opsec.

Switch to Linux

Operating systems like Windows and macOS collect large amounts of data. Linux is open source, meaning anyone can inspect the code. It has fewer built in trackers and gives you more control. Linux Mint is beginner friendly and can be installed from a bootable flash drive. Once installed, set up a firewall, your VPN, and secure browsers. Learning the terminal may feel strange at first but it gives you direct control over the system. Over time you will gain skills that help you stay ahead of threats. Linux is not magic but it removes many of the default problems of other systems.

Operational security is not a single tool or program. It is a mindset and a habit. By using a VPN, strong passwords, better browsers, and a secure operating system you reduce your exposure. The goal is not perfection but progress. The more you practice these habits the harder it becomes for anyone to use your data against you.