

OPSEC Guide

This guide is detailed but simple to follow, because protecting your security when reselling replicas as authentic items is absolutely essential. OPSEC and safety go hand in hand, and you can never be too careful. Once you finish reading this guide, read it again.

OPSEC, which stands for Operational Security, started in the U.S. military. It is a process used to prevent opponents from gathering information that could put a mission at risk. But OPSEC is not just for military operations. It is a key part of both defensive and offensive cybersecurity, and it is relevant to daily life too.

Keeping your identity private is something you have to work on all the time. You need to make sure your online traces, like your IP address, writing style, email accounts, habits, and language, cannot be combined to reveal who you are. It is not a one-time job; it requires constant attention.

There are many reasons why OPSEC matters. One of the biggest is your protection from hackers, cybercriminals, and even government surveillance. One of the main risks from bad OPSEC is getting doxxed, which is when your personal details get leaked and your safety is at risk.

Some people say, "If you have nothing to hide, you have nothing to fear." But the truth is, everyone has something they want to keep private. OPSEC is even more important when you are reselling replicas, since you are working in a grey zone. Keeping yourself safe and your tracks hidden is a must.

To stay unnoticed, you have to shield yourself from third parties. A VPN is a good starting point, but it is usually not enough by itself. The kind of protection you need depends on your activity. If you are just streaming from a sketchy site, a VPN might work. But for reselling, you need more layers of safety.

This guide introduces several essential apps that I recommend for staying safe online. I will explain what each one does so you can decide if it suits you. The goal is to make sure none of your accounts are connected. Platforms track more than your IP address; they also use browser cache and unique fingerprints.

Let's be honest. Everyone has files or accounts on their device that they want to keep private. Whether it's personal data or your reselling setup, it is important to protect it.

This guide will not just name tools. I will explain how to use each step so you can stay protected. Whether you are just starting or already experienced, you can never be too safe.

The tools you pick are your choice. You can keep it simple with a few core apps or go all in with a more complex setup for top-level protection. Either way, taking OPSEC seriously is always the right move.

Beginner Setup (Recommended):

1. Main PC
2. Encrypted Windows Drive
3. VPN
4. Privacy Browser

Advanced Setup:

1. Main PC
2. Encrypted Windows Drive
3. VPN
4. VMware
5. Proxy
6. RDP
7. Privacy Browser

I do not recommend using the advanced setup for reselling. Sites like eBay and PayPal can detect virtual machines or remote connections, and that can get your account flagged.

The beginner setup is not just for beginners. It is actually the best option for most resellers. The level of protection you choose should match your activity.

If you are doing something illegal (which you should not be), then you will need a much stronger setup to avoid getting caught quickly. The more protective layers you add, the harder it becomes for anyone to track you.

Watch Out

This part gives you a quick preview of what you will see next. Each tool below will improve your privacy and help keep you safe.

- **Encrypted Computer:** This is an essential tool for everyone concerned with privacy. It requires a password even before your system loads Windows, acting as a lock on your entire device. This security feature is extremely strong. Once set, not even advanced forensics or law enforcement agencies can break through it without the password.
- **VPN:** A virtual private network is another must-have. It protects your real location by assigning you an IP address from a different country. Since every website logs IP addresses automatically, using a VPN stops you from handing over your location each time you visit a site. It acts as a shield between your activity and anyone trying to trace it
- **VMware:** While it is not necessary for reselling, it is still useful to know about. VMware allows you to run a completely separate operating system on your computer, almost like having a second digital space. You can limit your reselling activity to this environment so that if anything goes wrong, such as malware or tracking, your main operating system stays untouched and safe
- **RDP:** Remote Desktop Protocol is another useful but optional tool. It lets you log into a different computer in another location, as if you were sitting in front of it. This can be handy for managing tasks without tying them to your main device. It generally costs about ten euros a month and works through a feature that already comes with Windows, making it easy to use without extra setup.

We will cover other useful tools later, but the most effective way to stay protected is knowing when to keep quiet.

Shut Up

This is the most important tip in the entire guide, which is why it comes before any technical advice.

Do not tell anyone in your real life what you are doing. Do not mention reselling. Do not show off your profits. Do not talk about it with your partner or your friends. The fewer people who know, the safer you are.

If you decide to tell someone close, only talk in person. Never use WhatsApp, calls, or any regular app to talk about this. Use apps with full encryption like Telegram or Keybase. If either of you is investigated and your chats are found, both of you could be in serious trouble.

If you trust someone online, do not give them your phone number, Snapchat, or anything that can be traced back to you.

If they get caught and your information is linked to them, you will be the next target.

Also, make sure that nothing you post online can be connected to your real identity. The easiest way to start is by using a different email for your reselling activities.

With that settled, let's move on to locking down your device and making your identity invisible.

Protect your PC

Antivirus

Let's begin with the basics. Antivirus software is not magic. It does not catch everything instantly. Some threats are FUD, which stands for Fully Undetectable. This means that even trusted antivirus programs may miss them for a few days before detecting and blocking them.

Whenever you download a file from an untrusted source, it is important to test it in a secure environment first. Sandboxie is a good choice for this. Even files like .png images, PDF documents, or Word files can contain harmful code. That is why you should always run a reliable antivirus program, even if you believe you can spot threats on your own.

Recommended:

Malwarebytes (Free)

Malwarebytes is well-known for its ability to detect and remove malware. It runs quietly in the background, scanning your system for harmful files and preventing many threats before they do any damage

VPN

You might think any VPN will do, but that is not the case. Sure, if you just want to view a website that is blocked in your country, almost any VPN can help. But when you are working with sensitive online activity, you need one that does not compromise your privacy.

A key feature to look for is a kill switch. This automatically blocks internet traffic if your VPN connection drops. Without a kill switch, your real IP could leak, making all your precautions useless.

Recommended:

MullvadVPN (€60/yr)

Mullvad is fast and well-respected. It is known for its strict no-logs policy and commitment to user privacy. Operating since 2009, Mullvad is one of the most trusted names in the space.

Proton VPN (Free | Basic €48/yr | Plus €96/yr)

Proton VPN comes from Switzerland, a country with strong privacy laws. It offers a free plan with limited features and two paid tiers for more speed and flexibility. It is a good alternative if you want privacy with flexible pricing.

Web Browsers

Your browser says a lot about you. Firefox is currently the best mainstream browser for privacy, especially when paired with the right add-ons. Here are some that you should definitely install:

1. uBlock Origin
Blocks unwanted ads and scripts. It is light on resources and highly customizable.
2. HTTPS Everywhere
Forces secure connections where possible. This helps prevent attacks during data transfer.
3. Oecentraleyes
Emulates content delivery networks locally, cutting down on unnecessary connections to third-party services.
4. ClearURLs
Cleans up tracking parameters from links automatically, reducing tracking across websites.

Private Email Providers

When it comes to email, you should stay away from providers that make money through ads or sell your data. Always choose one that puts your privacy first. Secure email services protect your identity and keep your conversations away from prying eyes.

ProtonMail

ProtonMail is based in Switzerland, which has some of the strongest privacy laws in the world. This service focuses on encrypted communication and gives you peace of mind knowing your messages are well protected. They have been running since 2013 and offer both free and paid options.

- Free version: Comes with 500 megabytes of storage, enough for basic use.
- Limitations: Free accounts cannot use certain features like the ProtonMail Bridge or advanced search.
- Paid version: Starts at 48 euros per year and gives you extra storage, custom domains, and added functionality.

Criptext

Criptext is another great choice for private emails. It does not store any of your emails on its servers and gives you full control over your data. Everything is encrypted on your device, so even Criptext itself cannot access your messages.

File Encryption Software

If your computer ever gets lost or taken, file encryption can protect all your data. When done properly, it makes your files completely unreadable without the password. This is one of the most important parts of OPSEC. Even if you are only mildly involved in reselling, it is still necessary.

You should encrypt every device you use, including desktops, laptops, and anything that might store sensitive info. It is a must if you want full control over your digital privacy.

Recommended: VeraCrypt (Free)

VeraCrypt is a free tool that lets you create encrypted spaces on your device. You can either encrypt just part of your drive or the entire thing. It also gives you the option to lock your system before Windows boots, so no one can access it without the password.

What does VeraCrypt do?

When you turn on your computer, VeraCrypt will prompt you for your password before anything else loads. If someone does not know the password, they will not be able to get into your data on the drive.

Why VeraCrypt?

- It's open-source.
- It's FBI-proof.
- It's widely trusted and has been audited for security.

It may take a bit of time to set up, but the steps are simple and easy to follow. The extra effort is worth it.

Password Manager Software

If you want to stay safe online, a password manager is essential. It stores your passwords securely and can generate strong ones so you do not have to remember them. Using the same password everywhere is dangerous, so this is a simple way to protect yourself.

If you are using Keychain, LastPass, or other similar services, it might be time to switch to something safer.

Bitwarden – Cloud (Free)

Bitwarden is a great open-source option. It keeps all your passwords safe and syncs them across your devices. You can use it on desktop, mobile, or browser.

Key Features

- Open-source and transparent.
- Syncs across all devices.
- AES-256 encryption for data protection.
- Free for basic use, with premium options for more features.

KeePassXC – Local

KeePassXC is similar to Bitwarden but does not connect to the internet. It only works on your computer, giving you more control and privacy. This option is great if you do not want your data stored online.

Key Features

- Open-source and highly secure.
- Offline use with no cloud syncing.
- Auto-type feature for browser login.
- Great for users who prefer local storage over cloud syncing.

Encrypted Instant Messengers

To keep your chats private, use messaging apps that encrypt everything from end to end. These apps make sure only you and the person you're talking to can read the messages.

Here are the best choices:

Telegram

Telegram is a widely used messaging app with a smooth interface and a large global user base. While it is convenient and has useful features, not all messages are protected equally. To ensure full privacy, you must use the "Secret Chat" feature, which provides end-to-end encryption. Regular chats are stored on Telegram's servers and are not fully private. The platform also logs your IP address and device info, and while they claim to only release data in serious cases like terrorism, this still leaves a gap in your privacy.

Keybase

Keybase puts privacy at the core of everything it does. It encrypts messages, file transfers, and team communications from start to finish. Not even Keybase employees can see what you send. It is especially useful if you need to handle sensitive files and verify identities securely. Whether you are collaborating or working alone, Keybase is a powerful tool for serious users who value digital protection.

Signal

Signal is one of the most trusted apps for secure messaging. Everything is encrypted by default—chats, voice calls, and attachments. It is open-source and regularly checked by security experts, which adds an extra layer of trust. Signal does not keep user data and stores almost no metadata. It requires just a phone number to sign up, and you can use a virtual one for even more privacy. For those looking for strong security without sacrificing usability, Signal is the top choice.

Your Personal Virtual Phone

When signing up for websites or platforms that ask for a phone number, avoid using your personal one. Instead, choose a virtual phone service that provides numbers you can use without revealing any of your real identity. These services help maintain your privacy and keep your main number disconnected from your reselling activities. Many of them let you choose from a variety of countries and offer numbers that are reusable and easy to manage.

Xootf

- Xootf lets you buy a phone number for long-term use. Unlike many free SMS services, the numbers here do not expire. You can use it for services like Telegram, marketplaces, or any site that asks for a number.
- Features
 - You can receive SMS on the number directly through their message panel.
 - Available for many EU, US, and UK numbers.
 - Completely anonymous purchase, so you can protect your real number while using it for services like Telegram or eBay.

Buying Extra SIM Cards

- You can also look for SIM cards that do not require ID. Local sellers or online platforms sometimes offer these. Depending on your country, you may find prepaid cards that let you activate and use them without any registration.

Why No Anti-Detect Section or Virtual Machine Section?

Anti-detect browsers used to be popular, but most of them just add a few tweaks on top of common browsers like Chrome or Firefox. They are not truly different underneath. Instead of relying on them, you can use Firefox with specific add-ons and custom settings to achieve the same level of privacy.

Proxies and anti-detect tools also come with risks. They are often flagged by platforms and can cause more harm than good. A better method is using different user accounts on Windows, rotating your IP, and keeping your setup simple but solid.

This is also why using virtual machines is not ideal. They do not behave like real devices and are easier to spot. Remote desktop tools have similar issues because the IP locations look suspicious to platforms.

Creating an Alter Ego

You do not need to rely on fake documents to protect your identity. A more practical and low-risk option is to use a slight variation of your actual name. For example, someone named Alex Walter might use a name like Alexander Walber. This keeps the name realistic and believable, but it cannot be directly traced to your real identity using common search tools or databases.

These name variations are especially useful when setting up email accounts or signing up for services. Most systems and platforms will still accept payments under a name that is close to the original, even if a few characters are changed. It is also much easier to make small edits to existing documents than to forge completely new ones, which reduces risk and effort.

This approach also works on platforms like eBay, where you can set custom usernames. While your real name may still be required for verification, the public-facing identity can remain separate. By using this tactic, you can maintain a convincing persona that helps protect your privacy without drawing unwanted attention.

Moving to Real-Life OPSEC

When meeting someone in person or shipping a product, there are still some rules to follow.

If you meet up with someone, use a backup phone or SIM card. Introduce yourself using your online alias. Never give out your actual name or personal ID. If someone insists on seeing ID, you can generate a fake one with tools like onetimes.org. After the meetup, avoid going straight home. Take a detour first.

For shipping, use a variation of your name and tweak the address if needed. You could slightly change the apartment number, as long as the package still finds its way to you. For more privacy, consider using a PO box or mail forwarding service.

What Should You Do at a Meetup?

If you are meeting a buyer in person, take extra precautions. Use a separate phone or SIM card that is not linked to your main identity. Always introduce yourself using the alias you use online. Avoid revealing your real name at any point, and never carry or show your actual ID.

In some cases, buyers may ask to see identification to confirm your identity. If that happens, you can use tools like onetimes.org to generate a temporary ID with a different name, a custom photo, and even an altered date of birth. This helps maintain the appearance of legitimacy while still protecting your real identity. If the deal is done in cash, that is even better—it leaves no digital footprint.

Once the meetup is complete, do not go straight home. Always change your route and stop somewhere else first, like a coffee shop or public place, before heading back. This adds an extra layer of privacy in case someone is watching or tracking you.

You Are Shipping Your Item

Shipping might seem less risky than meeting someone, but there are still important safety steps to take. Never put your full real name on a package. Instead, use a slight variation—just like you do online. You can also change small parts of your address, such as the apartment number, but only if you are sure the package will still reach you.

If you are worried about safety or do not want your home connected to your reselling activity, consider using a PO box or a mail forwarding service. These services let you receive packages at an alternative address, protecting your real location. Some even allow returns to be handled without ever linking back to your actual name or residence.

For shipping, use a variation of your name and tweak the address if needed. You could slightly change the apartment number, as long as the package still finds its way to you. For more privacy, consider using a PO box or mail forwarding service.

Exit Plan

You should always have an exit plan. Know where your data lives, and be ready to delete everything if needed. This includes files, accounts, messages, and your whole setup.

When it is time to step away, do a full cleanup. Leave no traces. Think of this as wiping the board completely clean.

Overview

Before we finish, it is important to remember that reselling replicas as authentic items exists in a legal grey area. You should always act with caution and avoid attracting attention. Be smart, stay private, and know your limits. Do not get carried away with greed. The more low-key you stay, the safer you will be.

The Basics of OPSEC in Reselling Replicas

What is OPSEC?

OPSEC is about managing the flow of information. If your personal identity or activities leak out, your entire reselling setup could be exposed. Good OPSEC protects your business and your privacy.

The Core OPSEC Principles You Should Follow While Reselling

1. Deterrence— Keep Things Quiet:

- **Acceptability:** Always aim to make your reselling activity look casual and unremarkable. If people notice what you are doing or your operation seems too flashy or bold, it may raise suspicion. Being low-key is what keeps you under the radar.
- **Credibility:** If someone begins to investigate your actions and finds parts of your setup that seem professional or organized enough to be legitimate, that alone could be enough for them to dig deeper. Avoid looking too structured, because even that can be a red flag.
- **Perception:** Keep everything vague. Avoid making statements or posts that could even hint at what you are doing. Make sure nothing in your digital footprint can be linked back to you directly. Do not use unique language, phrases, or branding that could identify you.

2. Detection— Avoid Getting Tracked:

- **Who:** Always operate under aliases. Make sure no real-life information—name, address, or ID—is connected to your accounts or operations. Use different aliases across platforms to prevent cross-linking.
- **What:** Be subtle in your actions. Avoid uploading large quantities of items at once, using flashy product descriptions, or advertising your service openly. These attract attention from both platforms and users.
- **How:** Rely on secure tools to mask your tracks. VPNs, privacy browsers like Firefox with the right extensions, encrypted messaging apps, and separate user profiles help keep your footprint hidden.
- **When:** Never develop a pattern. If you always ship or post on the same day, or log in at the same times, that consistency can be tracked. Randomize your actions slightly to make pattern recognition harder.

- Where: Don't keep all your inventory in one place, especially not in your home. Use variations of your address for returns if needed, and consider using PO boxes or drop points. Always ship from different places if you can.
- With Whom: Separate your personal and reselling connections entirely. Your buyers and suppliers should only interact with your online identity, not your real one. Keep communication in encrypted apps and never on platforms linked to your actual phone number or email.
- Why: Know your personal reason for reselling and keep it in check. If you try to scale too quickly or get greedy, you might slip up. Staying small, smart, and steady is safer in the long run.

How People Could Fight Back (What You Need to Be Ready For):

- Deception: Your buyers, competitors, or even law enforcement might try to pull some tricks to get information from you. Don't fall for it—keep your cards close to your chest.
- Neutralization: If they catch on to you, they'll try to shut you down. Be ready to erase all traces of your activity in case things go sideways. See exit plan.

How You Fight Back (Your Countermeasures):

- Cover: Always use a fake name and persona. Never tie your real self to the business.
- Deception: Mix it up. Use variations of your name and details that are harder to track. You want to make it tough for anyone to figure out who you really are.
- Conceal: Hide your tracks. The less information you leave behind, the better.
- Detection: Keep an eye out for any leaks or security issues. If something looks off, act fast.

The OPSEC Process: Prevent, Prepare, Respond, Recover

Prevent:

Do everything you can to control the information that leaves your system. Keep your setup minimal, safe, and anonymous.

Prepare:

Have plans in place for when things go wrong. Know how to delete accounts, switch devices, or cut off contact fast.

Respond:

If your privacy is compromised, react immediately. Shut down your operation, wipe data, and change all linked tools.

Recover: Start fresh using alternate tools, new profiles, and improved habits. Have backups and second options ready in advance.

Need to Know Principle:

Only share what needs to be shared. The fewer people who know what you do, the safer you are. Keep your real-life friends and online business contacts separate. Even within your reselling circle, limit how much information you reveal.

Methods for Keeping Track:

- Who knows what? Keep track of who has what info. If someone's getting too close to the truth, you need to know about it.
- Use strong encryption to protect anything sensitive, and make sure you've got backup plans in place in case something goes wrong.
- Always have a way to erase things quickly if you need to.

End Note, Thirteen Commandments:

- Never let anybody know your capabilities, your assets, your skills, your relationships.
- Never let anybody know your plans.
- Don't trust anybody.
- You're always under surveillance.
- Do not cache incriminating objects where you live or work.
- Keep operational activities and personal life strictly separated.
- Always clean up everything. Don't carry what you don't really need and know.
- Never mix activities, operations.
- Do not come into contact with the opponent. Do not talk with the opponent. Do not greet the opponent.
- Maintain your activities within your own skills, and the skills of your crew and contacts.
- Shut up.
- There is no break while you breathe.
- Everything leaves a trace.

The whole goal here is to keep everything hidden and secure. Stay smart, stay safe, and stay low-profile. If you follow these steps, you'll be able to run your reselling business without putting yourself at risk.