Digital Safety Basics for Activists and Organizers

A free community guide

You do not need to do everything in this guide. Doing some of it is dramatically better than doing none of it.

Introduction	Who this guide is for and how to use it
Section 1: Your Threat Model	Figure out what you are actually worried about
Section 2: Find Out What Is Out There	Search for yourself before someone else does
Section 3: Remove Your Data	The most impactful thing most people can do
Section 4: Lock Down Your Accounts	Passwords, two-factor auth, email, and social media
Section 5: What You Post and Share	You are the weakest link in your own security
Section 6: Secure Your Communications	Signal and encrypted messaging
Section 7: Device Security Basics	Your phone and computer
Section 8: Ongoing Habits	Security is not a one-time project

Introduction

This guide is for activists, organizers, journalists, advocates, and anyone who has been targeted online or is concerned they might be. It is written for people who are not technical. You do not need a background in computers or security to use it.

If you have been harassed, doxxed, or targeted before, start here. If you are publicly visible in controversial work such as organizing, advocacy, or journalism, start here. If you are a private person who just wants to clean up what is online about you, start here too.

What this guide covers:

- How to find out what information about you is already publicly available
- How to get your data removed from the sites that collect and sell it
- How to secure your accounts, email, and social media
- Why your own behavior online matters as much as any app or tool you use
- How to communicate privately
- How to keep your phone and computer from becoming your biggest vulnerability
- What habits to build so your security does not decay over time

What this guide does not cover:

- Advanced operational security for people whose physical safety is at immediate risk
- Organizational security assessments for groups or nonprofits
- Legal protections or what to do if you are being actively stalked or threatened

How to use this guide:

Start with Section 1. It will help you understand your own risk level, which determines which sections matter most to you. Then work through the sections that apply. You do not need to do everything. Doing some of this is dramatically better than doing none of it.

A note on perfection: Security is not a destination. Every step you take raises the cost and difficulty for someone trying to find or harm you. Do what you can, then do a little more.

> **The most important thing to understand before you read anything else:**
>
> No app, service, or tool is secure if the person using it is not careful. End-to-end encrypted messaging means nothing if you share sensitive information with someone you have not vetted. The strongest group security can be undone by one person who talks too freely, reuses a username, or lets the wrong person in. Every section of this guide covers tools and settings, but tools only protect you as far as your own habits allow. Your behavior is your most important security control.

Section 1: Understanding Your Threat Model

What are you actually afraid of, and who might be trying to find you?

"Threat model" is a security term that simply means: who might come after you, what do they want, and what is the realistic worst case? Different people face different threats. A journalist protecting a confidential source needs very different tools than someone who wants to remove their home address from Google. Knowing your threat model keeps you from over-preparing for things that will not happen while under-preparing for things that might.

Ask yourself these three questions:

1. Who might want to find or harm me?

An abusive or controlling ex-partner? A hostile online group or political opponent? A current or former employer? A government agency? Random harassment from strangers? Each of these operates differently and has different capabilities.

2. What do they want?

Your home address or current location? Your real name behind an anonymous account? Your private communications or contacts? Evidence of your activities or associations? Understanding what they are after tells you what to protect.

3. What is the realistic worst case?

Physical harm to you or someone you care about? Job loss or professional retaliation? Public doxxing and harassment? Being honest about this, without catastrophizing or minimizing, helps you prioritize.

What is your risk level?

Low risk: You want basic hygiene. You would like your personal information cleaned up from data broker sites. You have not been targeted before and are not in a high-profile or controversial role. Most of this guide applies to you. Start with Sections 2 and 3.

Medium risk: You have been harassed, doxxed, or targeted before, or you are publicly visible in controversial work such as organizing, advocacy, or journalism. Your identity, communications, or location could put you or others at risk. Work through this entire guide.

High risk: Your physical safety or the safety of people you work with depends on your anonymity. You are actively being targeted. You work in an environment with sophisticated, well-resourced adversaries.

> **Important:** This guide covers Low and Medium risk. If you are High risk, if your physical safety is at stake right now or you are protecting others whose safety depends on yours, please contact a professional. This guide will not be enough, and the wrong steps can create a false sense of security.

Section 2: Find Out What Is Already Out There

Before you can fix anything, you need to know what exists.

Most people are surprised by how much information is available about them with a simple search. The goal of this section is to see yourself the way someone trying to find you would.

Search for yourself

Open an incognito or private browser window and try the following searches. Using incognito prevents your own search history from shaping the results.

- Your full name and city, for example: Jane Smith Portland
- Your full name and employer
- Your full name and phone number
- Your username, if you use the same handle on multiple platforms such as Twitter/X, Reddit, Instagram, or gaming sites
- Right-click your profile photo and choose "Search image" to see where else that photo appears online

Write down what you find. This is your starting point.

Data broker sites

Data brokers are companies that collect personal information such as your name, address, phone number, and relatives' names, then sell it to anyone willing to pay. They get this data from public records, marketing databases, social media scraping, and purchases from other data brokers.

You almost certainly appear on several of them. The most common ones are Whitepages, Spokeo, BeenVerified, FastPeopleSearch, Intelius, and MyLife. Section 3 covers how to get your information removed.

For a complete list of brokers beyond the ones covered in this guide, see two free community resources: **privacyrights.org/data-brokers** (maintained by the nonprofit Privacy Rights Clearinghouse) and **github.com/yaelwrites/Big-Ass-Data-Broker-Opt-Out-List** (a comprehensive community-maintained list with direct opt-out links). California residents can also use the state's free DELETE Act platform at **cppa.ca.gov** to submit removal requests to every registered broker at once.

Check if your email has been in a data breach

Go to **haveibeenpwned.com** and enter each email address you use. This site, run by an independent security researcher and not a company trying to sell you anything, will tell you whether your email appeared in known data breaches. A breach means a company was hacked and your account information was stolen and often published online.

If your email appears in breaches, assume the password you used on that service has been exposed. Change it everywhere you reused it. Section 4 explains how to stop reusing passwords going forward.

What you probably cannot remove

Some information is a matter of public record: voter registration, court filings, property ownership, business filings. This is harder or impossible to fully remove. What you can do is limit future exposure by using a P.O. box for mail, keeping your name off property records where your state allows it, and being deliberate about what you post publicly going forward.

Section 3: Remove Your Data from Data Brokers

The most impactful thing most people can do.

Submitting removal requests to data broker sites is free and requires no technical skill. It takes time, figure on an afternoon to work through the major sites, but the payoff is significant. A motivated person trying to find your home address will hit dead ends instead of results.

Before you start

Create a simple notes file or spreadsheet to track which sites you have submitted removal requests to and when. You will need to revisit these every 6 to 12 months because some sites re-populate from public records. Start with whichever sites showed your current home address or phone number first.

Whitepages

- Go to whitepages.com and search for your name.
- Find your listing and copy the URL from your browser's address bar.
- Go to whitepages.com/suppression_requests and paste the URL.
- Enter your phone number to receive a verification text, then confirm.
- Allow up to 24 hours for the removal to take effect.

Spokeo

- Go to spokeo.com and search your name.
- Find your listing and copy the full URL of that specific page.
- Go to spokeo.com/optout and paste the listing URL.
- Enter your email address. You can use an alias for this; see Section 4.
- Click the confirmation link in the email Spokeo sends you.

BeenVerified

- Go to beenverified.com/opt-out/search.
- Search your name and find your listing.
- Select the correct listing and click "Opt Out This Record."
- Enter your email and confirm via the link they send.
- Allow 24 to 48 hours for removal.

FastPeopleSearch

- Go to fastpeoplesearch.com and search your name.
- Find your listing and click "Remove My Record" at the bottom of the page.
- Complete the CAPTCHA and confirm. No email is required.
- Removal is usually quick, within a few hours.

Intelius

- Go to intelius.com/opt-out.
- Search your name and select your record.
- Fill in the opt-out form and verify with your email.
- Allow up to 72 hours.

- Note: Intelius operates several related sites including PeopleLookup and iSearch. One opt-out request typically covers all of them.

MyLife

- MyLife requires a direct request by phone or email.
- Call 1-888-704-1900 or email privacy@mylife.com.
- Request removal of your profile and include your name and the URL of your listing.
- Follow up if you do not hear back within a week.

Google Search results

- If a page appears in Google results and you have had it removed from the source site, Google may still show a cached version.
- Go to google.com/search/howsearchworks/how-search-works/remove-information/ and use the "Remove outdated content" tool.
- This removes Google's cached copy only, not the underlying page.

For a longer list of brokers:

The sites above are the most common, but there are dozens more. For a comprehensive list with direct opt-out links, visit **github.com/yaelwrites/Big-Ass-Data-Broker-Opt-Out-List** or **privacyrights.org/data-brokers**. Both are free and maintained by privacy advocates, not companies trying to sell you a service.

Realistic expectations

Removals take anywhere from a few hours to a few weeks depending on the site. Some sites will re-populate your information from public records within 6 to 12 months. This is not a one-time fix. Set a calendar reminder every 6 months to re-check the major sites.

Automated removal services

Paid services submit removal requests on your behalf and monitor for re-population. None of them can remove truly public records, and all of them submit the same requests you could submit yourself. Whether they are worth the cost depends on how much your time is worth.

EasyOptOuts (about $20/year) is the most affordable option, Consumer Reports reviewed it favorably, and it rescans every four months. Independent testing found it clears roughly 65% of listings.

DeleteMe (about $129/year) has been around since 2011, uses human-assisted follow-up for sites that resist automation, and sends quarterly removal reports.

Kanary (about $180 to $200/year) also scans Google results and social media, which matters if doxxing is part of your concern. Backed by the Mozilla Foundation.

Privacy Bee (about $197 to $800/year) offers the broadest coverage but is out of reach for most people at the higher tiers.

This guide does not recommend a specific service.

Section 4: Lock Down Your Accounts

Controlling what you share and who can see it.

Passwords

Reusing passwords is the single most common reason people get hacked. When one site gets breached, attackers take those username and password combinations and try them on every other site: banking, email, social media, everything. If you use the same password in multiple places, one breach becomes a cascade.

The solution is a password manager. A password manager is an app that stores all your passwords in an encrypted vault, locked behind one master password that only you know. It generates a unique, random, unguessable password for every site you use. You only ever have to remember one password.

Recommended: Bitwarden (free)

- Go to bitwarden.com and create a free account.
- Choose a strong master password. Something long and memorable that you have never used anywhere else. Write it down and store it somewhere physically safe, on paper in your home, not digitally.
- Install the Bitwarden browser extension and the app on your phone.
- Start saving passwords as you log into sites. Over time, use Bitwarden to change old reused passwords to new unique ones. Prioritize email and banking first.

Two-factor authentication (2FA)

Two-factor authentication means that even if someone knows your password, they cannot get into your account without a second piece of verification that only you have. Think of it as a deadbolt added to a regular lock.

Text message codes are better than nothing, but they have a known weakness. Attackers can sometimes trick phone carriers into forwarding your number to their device, called a SIM swap attack. Use text codes if they are your only option, but upgrade to an authenticator app when you can.

Authenticator apps generate codes that change every 30 seconds and work offline. They are significantly more secure than text messages.

- **Aegis** (Android): free, open source, works offline
- **Raivo** (iOS): free, open source, works offline

To set up 2FA on an account, go to that site's security settings and look for "Two-factor authentication" or "Two-step verification." Choose "Authenticator app," scan the QR code with Aegis or Raivo, and save your backup codes somewhere safe.

Email

Most free email providers including Gmail, Yahoo, and Outlook scan your email to serve you ads and comply with government requests. For most people, this is an acceptable tradeoff. But if you need email that nobody else can read, including the company running the service, you need end-to-end encrypted email.

ProtonMail (proton.me) is the standard recommendation. It is free for basic use, based in Switzerland, and designed so that not even Proton can read your email. It works like normal email.

One important limitation: while your message content is encrypted and unreadable even to Proton, your account information is not. If Swiss authorities receive a valid legal request, Proton is required to hand over things like the IP address you logged in from, your account recovery email, and any payment information on file. This has happened to activists in documented cases. If you need to use ProtonMail with more anonymity, always access it through a VPN or Tor, and do not link a phone number, real recovery email, or payment method to the account.

Email aliases let you give out a different address for every service you sign up for, all forwarding to your real inbox. Data brokers and attackers who get one alias cannot connect it to your real address. **SimpleLogin** (simplelogin.io) is free, open source, and integrates with ProtonMail.

Social media

The most effective thing you can do is use social media less, or not at all, for anything connected to your activist identity. A profile that does not exist cannot be scraped, searched, or subpoenaed. If you participate in sensitive organizing, consider whether you need a public presence at all, or whether a private account with a small trusted audience would serve the same purpose.

If you do use social media, your profile should contain as little real information as possible. You are not required to use your legal name, your real photo, your actual location, or your real phone number on any of these platforms. Providing fake information to a social media company is not illegal. Using a pseudonym and a non-identifying photo significantly raises the cost of finding you.

Go through your privacy settings on every platform you use. What you are looking for: who can see your posts, who can see your friends or followers list, whether your profile is searchable by email or phone number, and whether your location is attached to posts.

Specific things to check on each platform:

- **Facebook:** Settings, then Privacy, then "Who can see your future posts?" Set to Friends. Check who can look you up by phone or email and set both to Nobody.
- **Instagram:** Settings, then Account Privacy, then set to Private if you do not need a public presence. Remove your phone number from your profile.
- **Twitter/X:** Settings, then Privacy, then uncheck "Let others find you by your phone number." Disable precise location on tweets.
- **LinkedIn:** Settings, then Visibility. Remove your phone number if it is listed.

Keep identities separate. If you do public activist work, think carefully about whether that public identity needs to be connected to your private personal accounts, your employer, your home neighborhood, or your family members' social media. Keeping them separate is not dishonest. It is prudent.

Do not reuse usernames

Using the same username or display name across platforms makes it trivially easy to connect your accounts to each other and to you. If you use one handle on Reddit and the same on Instagram, anyone who finds one has found both. Use different usernames for spaces where you want to maintain separation. When you need a new one, pick random words or a phrase from the nearest book rather than something personally connected to you.

Section 5: What You Post and Share

You are the weakest link in your own security.

> **No tool protects you from yourself.** End-to-end encryption, a VPN, a burner account: none of these matter if you share information that identifies you, your location, or your associates. The most secure app in the world cannot protect what you choose to say. And no group is more secure than its least careful member. If even one person in a network is careless about what they share or who they let in, that is the door that gets used.

What not to share

Personal details seem harmless in isolation but become identifying in combination. Someone piecing together your identity does not need your full name. They need enough overlapping details to narrow it down. The number of siblings you have, the year you graduated, your favorite local restaurant, the neighborhood you live in, the name of your pet: any of these alone is nothing. Several together can be enough.

In public or semi-public spaces, apply this standard: if you would not be comfortable with a hostile stranger knowing it, do not share it. Be vague about specifics. If you are proud of something you achieved, skip the identifying details. If you are going to an event, do not name it or describe who else will be there.

Images

Photos taken on smartphones embed GPS coordinates, device model, and timestamp data in the file by default. This is called metadata or EXIF data. Even if the photo itself does not show your location, the file carries it.

Before posting any image online, strip its metadata. ExifCleaner (exifcleaner.com) is a free tool that does this with a simple drag-and-drop interface. Make it a habit for anything you post in activist or organizing spaces.

Also: do not use a photo of your actual face as a profile photo in spaces where you are trying to maintain anonymity. If you want a profile image, use something from the internet such as an animal, object, or illustration. Strip the metadata from that image too before uploading.

Bonus tip: If you need to post real photos of yourself on personal accounts, the free tool **Fawkes** (sandlab.cs.uchicago.edu/fawkes) can alter images in a way that is invisible to the human eye but disrupts automated facial recognition systems. It does not make you anonymous, but it raises the cost of automated surveillance.

Links and tracking

When you share a link online, that link often contains tracking information that identifies where it came from, and sometimes which account shared it. Look for anything after a question mark in a URL. For example:

```
https://youtu.be/dQw4w9WgXcQ?si=qwertyuiop
```

The portion starting with the question mark is tracking data. Delete everything from the question mark onward before sharing a link. The link will still work. For an automated option, you can use linkcleaner.app.

When you receive a shortened link and cannot tell where it goes, do not click it without checking first. Use **ExpandURL** (expandurl.net) to see the full destination URL before visiting it.

Files

Do not open files from strangers or from sources you cannot verify without scanning them first. A malicious file can compromise your device even if you only open it to look at it.

- **Virustotal** (virustotal.com): paste a link or upload a file to scan it against dozens of security databases before opening.
- **Dangerzone** (dangerzone.rocks): a free tool that converts a potentially dangerous document into a safe PDF by stripping out anything that could run code. Useful for documents you need to read but do not fully trust.

Who you communicate with

Group security is only as strong as its weakest member. A Signal group, a private forum, a vetted organizing space: none of these are secure if they include someone who is an informant, an infiltrator, or simply someone who is not careful. Tools cannot solve this problem.

Be thoughtful about who you bring into sensitive spaces. Vet new members through existing trusted contacts when possible. Keep your most sensitive conversations to your most trusted, smallest group. What you would say publicly, say publicly. What you would not, protect accordingly.

> **A useful mental check:** Before sharing anything in an online space, ask yourself how you would feel if it appeared in a news story, a court filing, or a screenshot circulated by someone hostile to your cause. If the answer is uncomfortable, do not share it there.

Section 6: Secure Your Communications

Who can read your messages?

Regular SMS text messages are not private. They pass through your phone carrier, can be stored, and can be produced in court with a subpoena. Most messaging apps including Facebook Messenger, Instagram DMs, and Snapchat are also not private in any meaningful sense. The companies can read them, and so can law enforcement with a legal order.

Signal

Signal is the gold standard for private messaging. It is free, open source, independently audited by security researchers, and used by journalists, lawyers, activists, and security professionals worldwide. Messages sent through Signal are end-to-end encrypted, meaning only you and the person you are talking to can read them. Not Signal, not your carrier, not anyone else.

Encryption protects the contents of your messages. It does not protect you from your own words. Do not assume that using Signal means you can say anything. Use good judgment about what you put in writing regardless of the tool.

Installing and setting up Signal:

- Download Signal from signal.org or search "Signal Private Messenger" in your phone's app store.
- Register with your phone number. You can use Signal with your existing number.
- Go to Settings, then Privacy, and enable "Screen Security" to prevent screenshots of your conversations.
- Turn on disappearing messages for sensitive conversations. Open a conversation, tap the name at the top, and set a message timer. Start with one week for most conversations and shorter for sensitive ones.

Important notes about Signal:

- Signal calls are also encrypted. Regular phone calls are not. Your carrier logs who you call and when, even if they cannot record the content.
- Verify "safety numbers" with people you communicate with regularly. In a Signal conversation, tap the contact's name, then "View Safety Number." Compare it with them in person or over a trusted channel. This confirms you are talking to who you think you are.
- Both parties need Signal for the encryption to work. If you send a message to someone who does not have Signal, it sends as a regular SMS and will not be private.
- Signal is a tool, not a guarantee. The content of your messages is only as private as the people in the conversation.

What to do when someone will not use Signal

You cannot force people to use secure tools. Send them to signal.org with a one-line explanation. Accept that some conversations will happen in less secure channels and adjust what you say accordingly. Reserve your most sensitive communications for people who are willing to use Signal.

Signal vs. encrypted email: when to use which

Use Signal for real-time conversation, quick coordination, and anything that does not need a paper trail. Use encrypted email such as ProtonMail for longer communications, things you need to refer back to, or more formal exchanges. When in doubt, use Signal.

Section 7: Device Security Basics

Your phone and computer are the weakest links if not maintained.

Keep everything updated

Software updates fix security vulnerabilities. An unpatched phone or computer is an open door. Most successful attacks exploit vulnerabilities that already have patches available. Enable automatic updates on your phone and computer and do not keep dismissing the reminders.

Lock screen

Use a PIN of at least 6 digits. A pattern is weaker than a PIN because smudge marks on your screen can reveal it. Fingerprint and face unlock are convenient but can be compelled under duress or by law enforcement. A PIN requires a court order to compel in most jurisdictions. For higher-risk situations, consider disabling biometrics.

Full-disk encryption

Full-disk encryption scrambles everything on your device so that if it is taken from you, the data on it is unreadable without your passcode.

- **iPhone:** Encryption is on automatically when you set a passcode. Go to Settings, then Privacy and Security, scroll to the bottom, and it should say "Data Protection is enabled."
- **Android:** Most modern Android phones are encrypted by default. Go to Settings, then Security, then Encryption to verify.
- **Windows:** Go to Settings, then Update and Security, then Device Encryption. If BitLocker is on, you are set. If not, turn it on.
- **Mac:** Go to System Settings, then Privacy and Security, then FileVault. Turn it on if it is not already.

If your device is lost or stolen

- iPhone: go to appleid.apple.com and use Find My to lock or erase the device.
- Android: go to android.com/find and lock or erase the device.
- Change passwords to any accounts that were logged in on that device.
- Sign out of all other sessions by going to each important service's settings and using the "sign out everywhere" option.

Public WiFi and VPNs

Since most websites now use HTTPS (the lock icon in your browser), your traffic is encrypted even on public networks. Strangers on the same coffee shop WiFi cannot simply read what you are doing. The remaining risks: the network owner can see which sites you visit, and malicious hotspots can intercept less-protected traffic.

A VPN routes your internet traffic through a server run by the VPN provider, hiding it from your local network and internet provider. A VPN does not make you anonymous. The VPN provider can see your traffic instead, so what matters is whether they keep logs. Recommended options with strong no-logging policies: **Mullvad** (mullvad.net) and **ProtonVPN** (protonvpn.com). Both have free tiers.

Protests and high-risk events

If you are attending a protest or other event where there is a real possibility of device seizure or surveillance, the calculus changes.

- **Power off, do not just use airplane mode.** Airplane mode still leaves your data accessible to anyone who picks up your phone. Powering off and requiring a PIN re-entry at startup provides stronger protection.
- **Consider leaving your primary phone at home.** A cheap prepaid phone with only what you need that day limits what is at risk if your device is seized.
- **Understand what a burner actually protects against.** A burner phone protects your primary device's data. It does not make you anonymous to cell towers, which log which devices are present in an area. For true location anonymity, do not bring a phone at all.
- **Enable auto-wipe.** On iPhone: Settings, then Face ID and Passcode, then "Erase Data" after 10 failed attempts. On Android, this varies by manufacturer. Check your security settings.

Section 8: Ongoing Habits

Security is not a one-time project.

Everything you have done in this guide will decay over time if you do not maintain it. Data brokers re-populate. New breaches expose old passwords. Apps accumulate permissions. Your own habits drift. Here is how to keep it up without it taking over your life.

- **Every 6 months:** Re-run your name through the major data broker sites and submit new removal requests for any listings that have come back. Set a calendar reminder now.

- **Every 6 months:** Review app permissions on your phone. Go to Settings, then Privacy on iPhone, or Settings, then Apps on Android. Look for apps that have access to your location, microphone, camera, or contacts that they do not need. Revoke anything unnecessary.

- **When you move or change your phone number:** Audit where your old address and number appear and submit removal requests for any new listings that get created.

- **When you get a new phone:** Set it up fresh rather than restoring from a backup if possible. This clears out old apps and accumulated permissions. At minimum, review your app list and remove anything you do not use.

- **Before you share anything online:** Ask whether it could identify you, your location, or someone else. Strip metadata from images. Remove tracking parameters from links. Default toward sharing less.

- **Trust your instincts.** If something feels like it is exposing you, an app asking for permissions it has no reason to need, a service that seems to know too much about you, a conversation going somewhere uncomfortable: pay attention to that. You do not need to be technical to have good security instincts.

Closing: What This Guide Does Not Cover

This guide covers what a non-technical person can do for themselves. It is designed for Low and Medium risk situations. There is a whole other world of security beyond this, and if you need it, you will know.

This guide does not cover:

- Advanced operational security for journalists or activists in high-surveillance environments
- Organizational security assessments for protecting a whole group, not just yourself
- Device forensics and what to do if you believe your device has already been compromised
- Legal responses to stalking, harassment, or surveillance
- Protecting people whose identities must remain completely anonymous

When to seek professional help

You should contact a professional if:

- You are being actively targeted right now
- Your physical safety or someone else's physical safety is at stake
- You need to protect an organization, not just yourself
- You believe your device or accounts have already been compromised
- The stakes are high enough that getting something wrong would be catastrophic

---

Questions, complex situations, or need a hand? Reach out on Signal: **@Omega.50501**
