Doxxing Defense Checklist

ACTIVIST CHECKLIST

Last updated on **May 22, 2026** Takes about **45 minutes for baseline protections**

This copy was made on November 6, 2026. We update our guides often as threats change and as better ways to protect yourself become available. For the latest version, visit **activistchecklist.org/doxxing/**

Most online harassment campaigns start with publicly available data: your address from a people-search site, your photo from social media, your phone number from Venmo. The earlier you scrub yourself off the people-search sites, lock down social media, and use an alias for new sign-ups, the less attackers have to work with.

Doxxing occurs when harassers compile and publish personally identifying information about someone, with the intent to harass or intimidate them. It often leads to online harassment and can lead to lost jobs, legal consequences (we've seen ICE use compiled data to detain people), and in rare cases in-person harm.

The information revealed could include full legal name, home address, workplace, phone number, email, photos, family members, etc.

Why this is important: Our opposition uses doxxing and online harassment because they want to *create fear* that will cause us to stop doing our work. The more we take steps to defend ourselves in advance, the more powerful we can be in our actions. If you wait until after you've been doxxed, the information will already be out there and beyond your control.

How doxxing turns into harassment and harm

Examples of harassment that can result from doxxing: After your information has been shared, these are the kinds of harassment that could result: sending harassing emails/messages, trying to hack into your online accounts, sending packages to your address, impersonating you online, targeting your employer to hurt your reputation or get you fired, attempting to open credit cards in your name, providing your info to ICE or police to get you arrested, or attempting any of these attacks against your family/friends.

Most doxxing events stay online. The rare in-person escalations have included property vandalism, attackers showing up at your house or workplace to harass you, hiring a "doxxing truck[1]" to discredit you in public, swatting (calling a SWAT team on you), and most consequentially, government officials using the compiled data to detain people. These are unlikely unless you're a public figure.

Pathways an attacker could use:

- They could search for your name on search engines (like Google) or social media sites
- They could look you up on LinkedIn or find a copy of your resume to learn about your workplace, school, and professional history
- They could use photos you've posted online to infer information about where you live or places you spend time
- They could look you up on "people search" sites to get your address from your name or phone number
- They could look up your phone number on Venmo to see where you're spending time based on who you're paying and when
- They could use a photo of you (that they got online or took at a protest) to do a "reverse image search" to find your profiles online.

They can then share this information publicly in various ways: on public "doxxing sites" (ex Canary Mission[2], on social media, or in semi-public channels like Telegram and dark web forums.

How we can protect ourselves and our community

What we want to protect: Our goal is to make your personally identifying and sensitive information much harder to compile, starting with the highest-stakes pieces: your home address and workplace.

Do it together. Many groups doing public-facing work tackle this checklist as a security party[3] so everyone gets locked down at the same time.

We are in this work because we're committed to transforming systems and culture. It's easy to read guides like this and think "I need to hide everything and never go outside." That kind of fear is exactly what our opposition hopes will happen if they threaten us enough. Instead, we encourage you to use these defensive measures to empower you to **keep taking bold action**.

The more successful you are in your work, the more likely you are to eventually face some kind of doxxing or online harassment. Consider it a sign that you're on the right track.

Are you experiencing doxxing or online harassment right now? If so, jump to the doxxing response section below.

Baseline protections

EVERYONE This section is for you if you're doing any activism or advocacy that might attract the attention of your opposition.

See how easy it is to find your home address on Google using just your name or phone number

The best thing you can do to get a sense of how important it is to lock down your public profile is to search for yourself.

Later on in this guide, we will have you do a detailed manual Google search. But for now, **the purpose is just to learn what private information about you is easy to access**.

HOW TO DO AN INITIAL SEARCH ON GOOGLE FOR YOUR PRIVATE INFO - TRY TO FIND YOUR

Search Google for the following, replacing the example values with your real info:

- `"555-867-5309"` (your phone number)
- `"Jamie Garcia" address` (your name plus the word "address")
- `"Jamie Garcia" phone number` (your name plus the word "phone number")
- `"Jamie Garcia" "Springfield High School"` (your name plus your high school or college)
- `"Jamie Garcia" employer` (your name plus the word "employer," or try the name of your actual workplace)

Using quotes is helpful but not required. If you can't find anything, try without quotes.

Your task: **How long does it take you to find your home address?**

Most likely not very long. The rest of this guide will help you remove a lot of this information.

Important Remove yourself from "people search" sites using an automated service (like EasyOptOuts)

Using a tool to automatically remove yourself from all these sites saves a lot of time.

DO: Sign up for EasyOptOuts[4] ($20/year) — or Optery Ultimate[5] ($249/year) for more coverage

DO NOT: We don't recommend DeleteMe because it's less effective than EasyOptOuts

"People search" sites are a type of "data broker." They collect information from public and private records to form a "profile" for basically everyone. If you've ever had a phone number, used a credit card, or voted, you're probably on one of these sites.

Try it out: Search this site[6] for your name or phone number (we use this one as the example because it returns results immediately without making you sign up). Most people are surprised how much information is readily available. Other major sites in this category include Whitepages, Spokeo, BeenVerified, and a growing number of AI-powered lookup tools.

Why pay for automatic removal services: You can do this "opt out" process manually, but it takes an incredible amount of time, and you have to re-do it every few months when the data broker sites change. It's ridiculous that we have to pay to protect our privacy, but it saves a lot of time for us to focus on our organizing.

Which automatic removal tool should I use?

- **EasyOptOuts[4] (recommended)** - $20/year - It is among the most effective[7] and the cheapest.
- **Optery Ultimate[5]** - $250/year - Slightly more effective if you can afford the additional investment. They can take a copy of your ID (with ID number removed) and opt you out from sites that require an ID.
- **What about DeleteMe? -** It's the most well-known option, but it was only 27% effective at removing profiles compared to EasyOptOuts (65%) and Optery Ultimate (68%). (Source[8]).

HOW TO REMOVE YOURSELF FROM "PEOPLE SEARCH" SITES USING EASYOPTOUTS

Time required: 5–15 minutes

1. **Sign up for EasyOptOuts**[4] ($20/year)
2. **Enter your personal information:** Follow the prompts. It is most important to include your **current** information (address, phone number, email). If you can't find all your past addresses, that's okay.

   > **Warning:** Do NOT enter **alias names** or **burner phone numbers** that you use exclusively for activism that are already fully separated from your true identity. You wouldn't want those linked up inside this system.

3. Continue to the next checklist item to do **manual opt-outs** for the sites that EasyOptOuts can't handle.
4. Consider asking anyone who lives at your house to sign up as well. If someone finds out you live together, they could look up that person just as easily and then target you.

Timing: It can take a few days for the initial removals to complete and sometimes up to a couple of months for certain sites.

FYI: We don't get any commissions for any paid services we link to. We recommend them because they're the most effective ones we've found.

EasyOptOuts Privacy: Some people are concerned about entering all their information into a site like this. While no site is immune to data breaches, we trust this site based on their history and reputation. And the information is necessary to do removals.

Alternate tool: Kanary[9] is a free app that searches Google for your personal info and walks you through manually removing it. It is still very time intensive and people are likely to abandon it before they finish all the removals.

Important **Manually opt-out of "people search" sites that aren't covered automatically**

Even the most effective "people search site" removal tools only cover 70% of the sites.

Some of these sites make it very difficult to remove a profile, so services like EasyOptOuts can't do it for you. These usually require you to receive an email to confirm you are the person removing the profile.

HOW TO MANUALLY REMOVE YOURSELF FROM HIGH-RISK PEOPLE SEARCH SITES

Start by manually opting out of the most high-risk sites:

1. **Opt-out of People Connect (Intelius)**[10] - They own many people search sites, so one opt-out goes a long way. Fill out the "suppression form." You will be asked to verify your email/phone.
   - If the site asks you to verify a phone number or email that you don't have access to, call their technical support (877) 564-3253 and request to have your "personal information suppressed." Calling is much more effective than emailing them, in our experience.
2. **Search for yourself on National Public Data**[11]**.** If you find a result, scroll to the bottom of the page and click Do Not Sell My Info to opt-out[12].

There are other sites you'll only find by searching for your info manually on Google (explained in a later checklist item).

Fully manual: If you would like to do all of the opt-outs manually, you can use Yael Grauer's Big Ass Data Broker Opt-Out List[13]. Services like EasyOptOuts handle most of these for you, but not all of them. You could use this list to manually do the process at no cost, or manually search each database to see what you've missed.

Opt-out of "face search" sites

Protect yourself from a photo being used to find your identity.

You can protect yourself by opting out of "reverse photo search" sites. This makes it harder for someone to use your profile picture online to find out your legal name, which can lead to them finding you on the people search sites mentioned above.

HOW TO REMOVE YOURSELF FROM "FACE SEARCH" SITES

Each of these sites will (ironically) require you to upload a headshot. This is a necessary evil if you want to be removed. You have to decide if the risk of giving them more data is worth the payoff of being opted out.

> **Note about uploading your government ID**: Some of these sites are awful and require you to upload a photo of your government ID or passport with sensitive information hidden. The easiest approach is to put tape over everything on your ID except your name and photo, then take a picture.

Sites to opt-out from:

1. Opt-out of Clearview.ai[14] - Only requires a photo, not a government ID. Frustratingly, opt-outs are only possible in states that have passed privacy laws. ***Clearview is used primarily by law enforcement agencies, so it is important to opt-out of.***
2. Opt-out of PimEyes[15] - Requires a photo of your government ID. (Block out your ID number!)
3. Opt-out of FaceCheck.ID[16] - Instead of uploading a government ID, you can upload a selfie you take with two fingers touching your chin. Also, you must manually select which photos you want them to remove.

Enable Google's "Results About You" notifications

This can help you stay notified about pages that have your personal information.

Google offers Results About You[17] as a tool to help you know when your private information is shared online. It's not the most helpful in removing those results, but it will help you know when you need to manually find ways to get the information removed.

HOW TO ENABLE GOOGLE RESULTS ABOUT YOU

1. **Enable Google "Results About You"**[18]: Fill in your full name (and any other names you use), addresses, phone numbers, and email addresses.

   > **Warning:** Do NOT enter **alias names** or **burner phone numbers** that you use exclusively for activism that are already fully separated from your true identity. You wouldn't want those linked up inside Google's systems.

2. **Wait** for the initial scan to complete (a few hours)
3. **Review the results and find ways to get them taken down:**
   1. Using the "request removal" button inside Google's tool is usually not helpful for two reasons: 1) Google will deny most requests unless they are from a "people search" site or intentional doxxing. And 2) the original information is still out there even if Google does remove it. People can find it on other search engines or the original site directly.
   2. Instead, you want to try to contact the site owner to get the information removed. On websites, this means finding a contact form/email and telling them the page that has information you're asking to have removed. On social media sites, this might mean removing a post you made or asking the author to remove it.
   3. Click "mark as reviewed" as you handle each item.
4. **Submit a Google "removal request":** Use this removal request form[19] to ask Google to remove search results that have your personal information or other doxxing content. This is different than Google's "Results About Me" feature.
5. **Watch for notification emails** about new results as they come up. You'll usually see the most in the first couple weeks after you sign up.

Privacy: Requires a Google account. There is a trade-off here: you're handing Google additional identifiers like your other names, phone numbers, and addresses, which they'll then have on file linked to your account. The trade-off is usually worth it because Google already has most of this information about you, and the upside is getting notified when your address or other private info shows up somewhere new on the web.

☐ Lock down the privacy settings on your social media accounts

Most of us shared a lot more information about ourselves on social media before we started wanting to protect our privacy.

Locking down our social media profiles can take a long time.

Things you might want to protect: Your location, your email address (can be used to search for you even if it's hidden), your friend's list, your workplace, your full birthdate (can be used to gain access to other accounts like your bank), and photos/posts that show where we spend time most often.

Being bold and public vs private: Some people have intentionally public profiles with a following that they want to keep because they're using it for their activism and organizing. For example, they may choose to keep their profiles accessible while others might choose to hide their profile, so only friends can see it.

OPTION 1: HOW TO LOCK DOWN YOUR SOCIAL MEDIA PRIVACY SETTINGS WITH BLOCK PARTY

While you can do this manually (see below), we recommend using Block Party[20] because it will help guide you through which privacy settings to change. It will help you lock down Facebook, LinkedIn, Instagram, X/Twitter, TikTok, Snapchat, Reddit, Strava, Venmo, Google, Google Maps Reviews, YouTube, and Bluesky. The free tier is helpful, and we've reviewed their privacy policy and generally trust the creators.

1. **Install the Block Party extension**[21] (free) for your browser. (This is a great time to install Brave[22] if you haven't yet!) Follow the installation prompts.
2. **Press "Start Scan"** and select which social media sites you use. Let it run for a few minutes while it checks all your settings.
3. **Next to each site, click on "To Do"** to see the recommended changes. You can start doing this manually or have Block Party automate a lot of them.
4. **You can automate a lot of the changes:** Block Party will make 50-70% of the settings changes for you automatically. This requires either a 7-day free trial or a paid account ($50/year if you use the promo code JOINTHEPARTY — we don't get any commission).
5. **Do the remaining manual changes:** Follow the "To Do" lists for each site that can't be done automatically.
6. Finally, consider what other social media sites you use that might not be covered by Block Party: Cash App, Venmo (if not already covered), Partiful, Nextdoor, AllTrails, Strava, Pinterest, Goodreads, MapMyRun, dating apps, etc.

If you want to delete your old X/Twitter posts or migrate to Bluesky, check out Cyd[23].

OPTION 2: HOW TO MANUALLY LOCK DOWN YOUR SOCIAL MEDIA PRIVACY SETTINGS

If you don't want to use Block Party, you can do the following steps with each of your main social media accounts.

Sites you might want to prioritize (roughly in order of risk):

- Facebook
- LinkedIn
- Venmo
- Cash App
- Google Maps Reviews
- Yelp
- Strava
- All Trails
- Instagram
- X/Twitter *(To delete your old posts, check out Cyd[23].)*
- Bluesky
- YouTube
- TikTok
- Snapchat
- Reddit
- Partiful
- Nextdoor

Steps for each site:

1. **Consider deleting this profile** if you don't need it anymore. Many sites (Facebook, Instagram, Google) let you download a copy of your data first so you don't lose photos or messages. If you delete it, you're done. If not, proceed.
    - **Need just Facebook Marketplace?** Consider creating a separate dummy Facebook account for Marketplace use, then deleting your main one.
2. **Find the privacy settings screen** and change all the settings to be as private as possible.
3. **Remove your city**
4. **Hide your friends list**
5. **Prune your followers/connections.** Remove people who don't have at least one or two friends in common with you, especially if you don't actually know them. Even on a "private" profile, anyone you've accepted as a follower can still see and screenshot your posts.
6. **Remove old posts and photos** that share detailed information about where you live, where you spend time, and who you spend time with.

Consider using Digital Footprint Check[24] with usernames you commonly use to see where you might have profiles that you've forgotten about.

☐ Wear a mask when encountering cops or right-wing adversaries

This helps protect you if a bad actor tries to use your face to uncover your identity

Police and ICE use facial recognition against dissidents[25].

Right-wing adversaries often photograph protesters to run reverse image searches and identify participants—some maintain databases like Canary Mission[26] with activist profiles. Hiding some or all of your face makes this harder.

A KN95 mask can help you avoid facial recognition tools. It's not perfect (some tools only need your eyes), but it helps significantly.

Other identifying features matter too. A face covering alone isn't enough if other parts of you are easy to recognize. Adversaries often identify masked protesters by their distinctive tattoos, hair color or style, body shape, skin tone, and clothing, especially when several of these are combined. Consider covering visible tattoos with long sleeves, wearing a hat or hood, and rotating your protest clothing if you want to be harder to track across actions.

> As with other items on this list, privacy and visibility can be in tension: some may want to minimize risk by covering their face and eyes, while others prefer showing their full face to build trust and convey emotions more directly.

Legal note: Some cities have passed anti-masking laws that make it illegal to wear a mask. You may want to check your local city ordinances.

☐ Complete our Digital Security Essentials checklist

This guide covers other important doxxing protection steps like passwords, app location permissions, and software updates.

If you're concerned about doxxing, it's a good idea to complete the steps outlined in our Digital Security Essentials checklist →[22]

Many of these will protect you against someone trying to access your accounts or devices if you're the target of doxxing.

These items from the Essentials checklist are especially important:

- **Turn off location tracking** for most apps
- **Install the latest software updates** for your laptop, phone, and apps
- Use a **password manager**
- **Change your existing passwords** if they are weak or reused across multiple sites.
- Enable **two-factor authentication** on your important accounts
- Don't click on **suspicious links**

☐ Don't use your real name or photo on your Signal profile

Helps protect you from cops or attackers who want to de-anonymize you. Especially useful if you are in unvetted Signal groups.

A lot of community organizing happens in unvetted groups on Signal where you don't know how much you can trust everyone in the group. These groups can be infiltrated by right-wing adversaries[27] and law enforcement[28].

Using a fake name prevents someone from finding your real identity through a Google Search.

Using a photo that isn't your face prevents someone from finding your social profiles based on an image match or facial recognition.

Both steps help defend you against doxxing[29] and online harassment.

HOW TO CHANGE YOUR PROFILE

1. **Change your profile display name:** Open Signal → Tap your profile picture → **Settings** → Tap on your name/icon near the top → Click the top item with the silhouette of a person → Edit your profile display name
2. **Change your profile photo:** Open Signal → Tap your profile picture → **Settings** → Tap on your name/icon near the top → **Edit photo** → upload a generic photo that you found online that doesn't relate to your identity/preferences/interests/location.

The same principle applies even more strongly to social media. If your Instagram, Facebook, or LinkedIn profile pairs your full real name with a clear photo of your face, attackers can easily identify you even if the rest of your profile is private. See Lock down social media for more.

Remind people in your groups to do these things too. Security is a team sport.

Enhanced protections

MEDIUM-THREAT This section is for you if you're in a visible role related to your political dissent.

Configure Signal so your phone number is not discoverable

Even though your phone number isn't visible on Signal by default, people can still type in your phone number and find you. If you're at risk of harassment, you may want to only share your Signal username[30] with folks instead.

HOW TO MAKE YOUR PHONE NUMBER NOT DISCOVERABLE ON SIGNAL

1. **If you want to change your username:** Open Signal → Tap your profile picture → **Settings** → Tap on your name/icon near the top → Tap the **@** symbol → **Edit username** → set the username to something **completely unrelated** to your identity, or any usernames you've used anywhere before. It must end in at least 2 numbers.
2. **Hide your phone number:** Open Signal → Tap your profile picture → **Settings** → **Privacy** → **Phone Number** → Under **Who Can See My Number** → Select **Nobody**.
3. **Make your phone number not discoverable:** Open Signal → Tap your profile picture → **Settings** → **Privacy** → **Phone Number** → Under **Who Can Find Me By Number** → Select **Nobody**.
4. Tell people your username instead of your phone number when you want to connect with them on Signal.

Get an alternate phone number instead of sharing your primary number publicly

Your phone number can be a quick way for people to find your home address using "people search" sites.

DO: Use Google Voice[31] (free, less private) or MySudo[32] ($2/mo, more private)

DO NOT: Share your phone number publicly online or in large unvetted spaces

Sharing your primary phone number publicly not only puts you at risk of harassing calls/texts, but if any of the "people search" sites haven't removed you, someone could use your phone number to find your home address.

HOW TO SET UP ALTERNATE PHONE NUMBERS

- **Get an alternate phone number** if you need to share a phone number publicly.
  - Google Voice[31] is free, but Google is where the cops will go first to subpoena information, so it's the least private option.
  - MySudo[32] is $2/month for 100 texts and 30 minutes of calling.
  - Sideline[33] ($15/month) or Line2[34] ($10/month) if you need unlimited texting/calling
- **When you need people to contact you on Signal, tell them your Signal username**[30] instead of your phone number. (Of course, use Signal[35] whenever possible, especially when organizing. And make sure to turn disappearing messages on by default in settings.)

Ask people you live with to scrub their private info from "people search" sites

Everyone in your house needs to protect their info if you want your address to be private.

One of our main goals is to protect your home address from bad actors.

A motivated attacker might be able to find out who you live with through social media posts, friends lists, or family tree sites. If you've removed yourself from people search sites but your housemates or family members haven't, the attacker might still be able to find your home address.

Family members who share your last name are an especially strong link, since attackers can pivot from any one of them straight to your shared address on the "people search" sites.

HOW TO SUPPORT THE PEOPLE YOU LIVE WITH TO REMOVE THEIR PRIVATE INFO

1. **Ask each person** you live with to remove their private info from "people search" sites. Example text/script:

   > I'm working to remove our home address and my other private info from the internet, so we are more protected. Can you take a few minutes to do the first two items on this checklist so our address isn't easy to find online: https://activistchecklist.org/doxxing[36] I'm happy to sit down and do this together if you have time this week.

2. If it's helpful, you can search for your address on Google and find specific pages where their name is attached to the address. You could send them the link to this page to help show why it's important. Most people are surprised to discover how easy it is to find information like this online.
3. **Set a reminder** to follow up with them in a week or so to see if they need any support.

You might also make the same request of people who used to live with you at your current address, since their former address is still on "people search" sites.

Do a manual Google search for your private info

There are always going to be results you have to find and remove manually.

If you only rely on automatic data removal tools like EasyOptOuts, there will likely still be a lot of results that show your private info.

We're most concerned with removing your current home address and, secondarily, your phone number. Your email might be public and lead to harassment, but it's easier to manage.

The Kanary app[9] (free tier) can help you do some of this searching work.

HOW TO FIND AND REMOVE YOUR PERSONAL INFO ON GOOGLE

1. **Do separate google searches for your info.** Use quotes around your search to get more accuracy. Scroll through the first 2–3 pages on Google for each search (don't use Brave Search or other privacy search engines for this task).
   - **Home address in quotes:** `"742 Evergreen Terrace, Springfield"` or even just `"742 Evergreen Tr"` though that may turn up too many results that aren't in your city.
   - **Phone number in quotes:** `"555-867-5309"` or `"5558675309"` or `"(555) 867-5309"`
   - **Full name plus city (each in separate quotes):** `"Jamie Garcia" "Springfield"`
   - **Just your full name in quotes:** `"Jamie Garcia"` (will produce a lot of results that might not be you)
2. **Keep a list** of what you find that includes your sensitive private info. Prioritize sites that list your address or phone number.
3. **Make a plan to get each one removed.**
   - If it's a "people search" site, look for a "do not sell my info" or "opt out" form to fill out.
   - If it's a social media site, the author needs to remove it. Or you can try to press "report content" if they're unwilling to remove it.
   - If it's some other site, look for a contact form and ask them to remove it because you're concerned about being the target of online attacks. Most sites are willing to help.
   - **Ask search engines to remove the result.** For harassment, doxxing, or other harmful content, you can submit a removal request directly to Google (form[19]) and to Bing (form[37]). Success rates vary, but it's worth trying for the most harmful results.
4. **Set a reminder to check back in.** Check in after a week. If you didn't hear back from any of these sites, try to follow up.
5. **Set up Google Alerts**[38] for each search above so you're notified when new items come in. (Google's "Results About You" is good but it definitely misses things.)
6. **Refresh the Google results.** If you got a listing removed on the source site, but it's still showing up in Google's results, you can request the content be updated[39].
7. **Try other search engines too.** Different search engines surface different results, and an attacker isn't limited to Google. Run the same searches on Bing and DuckDuckGo to see what else turns up.

☐ Freeze your credit reports

Protects against someone trying to open credit cards in your name.

A bad actor might try to open credit cards in your name, which can damage your credit score and create long-term financial difficulties.

Freezing your credit report prevents anyone from opening cards/loans in your name. You can temporarily unfreeze it when you need to.

HOW TO FREEZE YOUR CREDIT REPORT

You must manually place a "freeze" on **all three** of the credit bureaus:

- **Equifax**[40]
- **Experian**[41]
- **TransUnion**[42]

This is always free. Don't accept any paid offers they make.

You will need to remember to temporarily lift the freeze when you need to run a credit report to open a new account in the future.

Blur your house on Google Maps and Apple Maps

This makes it harder for a bad actor to know the layout of your house/yard.

If a bad actor can get ahold of your address, they might try to find your house on Google Maps if they intend to harass or harm you in-person. Or they might be able to learn things like what kind of car is parked in your driveway.

HOW TO BLUR YOUR HOUSE ON MAP SITES

Note: You cannot undo a blur once you request it. For most folks, there's very little upside to having your house visible on street view.

Blur your house on Google Maps (details[43]):

1. Find your home on Google Maps[44].
2. Open the Street View image that you want to blur.
3. In the bottom right, click “Report a Problem” and complete the form indicating that you want to blur your house for privacy reasons.

Blur your house on Apple Maps:

1. Email mapsimagecollection@apple.com. Include your home address and explain that you'd like it blurred for privacy reasons.

Remove your house from real estate sites (Zillow, Redfin, etc.)

Hiding photos of the inside of your house helps keep everyone safer.

Zillow, Redfin, Realtor.com and others often show not just the outside of your house (which presents some risk) but can show a detailed layout of the inside of your house. This can give the opposition information that might help them harass or harm you.

You can protect against this by requesting the images be removed for your address.

HOW TO REMOVE IMAGES OF YOUR HOME FROM REAL ESTATE SITES

If you do not own the home, you may need to ask your landlord to do these removals since they require an account on each site. They have to "claim" the house on each real estate site.

You can also first search on the site to see how detailed the photos are and whether you want them removed.

1. Remove from Zillow[45]
2. Remove from Redfin[46]
3. **Realtor.com**: Log in → **Claim Home** → **Edit Photos**
4. Ask your real estate agent to remove the photos from the MLS so they disappear from any other sites.

Enable Lockdown Mode (iPhone) or Advanced Protection (Google & Android)

Spyware is an advanced type of attack, exploiting sophisticated vulnerabilities on our devices. In response, Apple and Google have introduced an advanced security mode that offers enhanced protection against spyware.

On iPhones, it's called **Lockdown Mode**[47] and on Android, it's called **Advanced Protection Program**[48]. (You can also enable Advanced Protection Program on just your Google Account even if you don't have an Android phone.)

We have **no reports** of anyone getting infected with spyware who had Apple's Lockdown Mode enabled. Android's Advanced Protection is more recent and its effectiveness has yet to be tested.

Usability trade-offs: Both features come with some functionality sacrifices. See the full list of trade-offs[49]. If you encounter issues that don't work for your needs, you can always disable the feature later.

HOW TO ENABLE LOCKDOWN MODE FOR IPHONES

IPHONE

Settings → **Privacy & Security** → **Lockdown Mode** → **Enable**

This feature is available for iOS version 16 and above.

HOW TO ENABLE ADVANCED PROTECTION ON ANDROID

ANDROID

Settings → **Security & Privacy** → under **Other Settings** tap **Advanced Protection**

Note: The location of this setting may vary between Android devices, so we recommend searching for 'Advanced Protection' in the Settings search bar.

This feature is available for Android 16 and above.

Enable Signal PIN and Registration lock

Protects you from advanced attacks where someone "steals" your phone number and registers it on Signal

If a highly-motivated attacker is able to find out your phone number, they can attempt to take it over through something called "SIM Swapping" or by calling your service provider and initiating a phone number "port" to a new provider. They could then use your phone number to register a Signal account and start receiving messages meant for you.

These are advanced attacks that don't happen to most folks. Still, it is easy to protect your Signal account.

You can protect yourself by enabling **registration lock** on Signal. It prevents someone from hijacking your account even if they steal your phone number. No one will be able to register a new Signal account on your number until your account has been inactive for 7 days.

If you forget your PIN, you will have to wait 7 days before you can create a new account (and your contacts will not be recovered). More on PINs & registration lock[50].

HOW TO ENABLE SIGNAL PIN AND REGISTRATION LOCK

Enable registration lock: Open Signal → Tap your profile picture → **Settings** → **Account** → Enable **Registration Lock**

Upgrade your PIN: You had to set a Signal PIN during setup. If you don't remember it or want to use a stronger PIN, here's how you can do that:

1. **Generate a strong PIN:** For maximum security, use a PIN that is 8 or 10 digits and make sure it is computer-generated. Here's a random PIN generator[51] you can use.
2. **Set a Signal PIN:** Open Signal → Tap your profile picture → **Settings** → **Account** → **Create/Change PIN** (If you don't already know what your PIN is).
3. **Save your PIN or enable PIN reminders:** If you have a password manager[22] you use reliably, save your PIN there. If you think you might forget where you saved your PIN, leave "PIN reminders" enabled.

High-profile protections

HIGH-THREAT This section is for you if you might end up receiving major media attention related to your dissent or your adversaries have a lot of resources.

☐ Invest in advanced data removal services (ex: Optery Ultimate)

If you're at very high risk of being attacked for your politics, you'll want to make sure you've done a thorough job scrubbing your data online.

Start by upgrading your automated data removal tool from EasyOptOuts to something like Optery Ultimate[5] ($250/year). It is among the most comprehensive automated opt-out tools. You can also consider Kanary Pro plan[9] ($10/month) for some additional coverage.

Depending on your risk level, you may want to invest in a high-end service that can do thorough data scrubbing for you.

Activist-aligned data scrubbing and doxxing response services:

- Brightlines[52]
- Convocation Research & Design[53]

You can also check out the Access Now Helpline[54] which is usually free, but much slower and less thorough.

☐ Do an advanced social media scrub and lockdown everything

The basic social media lockdown steps above are a good start. If you're at high risk of being targeted, you should do a more detailed scrub.

HOW TO DO A DETAILED SOCIAL MEDIA SCRUB AND LOCKDOWN

1. Make a list of every site where you have or had a profile, even ones you haven't used in years. Think beyond the big platforms: dating apps, fitness apps, review sites, payment apps, and old forums all count.
2. Search for your common usernames on Digital Footprint Checker[24] and Instant Username[55] to find profiles you forgot about. Add them to your list.
3. Go through your list and do these steps on each site:
   - Delete the profile if you don't need it anymore
   - Change your display name
   - Change your username
   - Remove your profile picture
   - Remove your location from your bio
   - Hide posts and photos that might reveal your location
   - Hide your friends list
   - Change your email address (consider DuckDuckGo Email Protection[56] or the Gmail "plus trick"[57]).
   - Change your privacy settings.
4. This may take many hours to complete. Check off each site as you finish it so you can pick up where you left off.

Tip: You can use this identity generator[58] if you need a random display name, username, or profile picture.

☐ Set up a PO box so you can stop giving out your home address

DO: Set up a PO box[59] or mail forwarding/scanning service like iPostal1[60]

DO NOT: Keep giving people your street address

You may want to stop giving out your real street address when registering for services, getting packages delivered, etc.

Options:

- **PO box with USPS**[59]: The main downside is that FedEx and UPS will not deliver to a PO box.
- **UPS Mailbox**[61]: More expensive, but accepts mail from USPS and FedEx, while also maintaining increased privacy.
- **iPostal1**[60]: Gives you mail scanning + physical pickup, and it also allows delivers from all shipping services (including FedEx and UPS) that won't always deliver to PO Boxes. Comes with a privacy risk if their services are ever breached, or they get a court order to turn over data about you.

Note: UPS Mailbox and any "virtual mailbox" service like iPostal1 that you use will require you to provide government ID and sign a form (USPS Form 1583) that is submitted to USPS.

☐ Use a unique identity for every online account you make (name, email, username, phone number)

Instead of signing up with your real name/email/phone/etc., you can start using **random, unique identities for each account**.

This makes it harder for attackers (and tech companies) to link your accounts across sites and create a profile from all those bits of information.

HOW TO USE A UNIQUE IDENTITY FOR EACH ACCOUNT

Make sure each of these is unique for each site, whenever feasible:

- **Display name:** Use this random identity generator[58].
- **Username:** Use this identity generator[58] or this specific username generator[62].
- **Profile photo:** Leave it blank or use this identity generator[58]. If you use the same photo on all sites, an attacker can do a "reverse image search" to find all your accounts.
- **Email address** - Use an email alias service like:
  - Qwacky to use @duck.com email alias[63] (free, Chrome/Firefox extension)
  - Proton Mail[64] (free/paid)
  - Addy.io[65] (free/paid)
- **Phone number:** Try to just not enter a phone number when prompted. If you need to enter a phone number just for verification when you sign up, try renting a phone number from SMSPool[66] ($0.50 per registration). If you need a long-term phone number, consider MySudo[32].

☐ Help the people around you defend their private info (family, friends, co-workers, comrades, neighbors)

If you are a high-risk target, you should evaluate the likelihood that others in your life might be targeted as part of harassing/harming you. This is very common when an activist makes front-page news. Right-wing trolls and vigilantes will go after family members, housemates, friends, co-workers, comrades, neighbors.

Message people in your life and suggest they do at least the first section of this guide.

Here's the link to the checklist you're currently viewing: https://activistchecklist.org/doxxing[29]

Having these conversations can be challenging sometimes (especially with family members). It may take time to explain to someone why they are at risk because of actions you are taking.

You may also want to inform your employer (and any coworkers who handle communications, like a receptionist or HR contact) in advance that you are at risk for harassment, so they understand the scenario if they get suspicious or concerning calls or emails about you.

☐ Make a personal emergency plan in case you are threatened at home

The highest level of attack from doxxing involves someone finding you in-person at your home or in your life to harass, threaten, or attempt to harm you.

Follow our Personal Emergency Planning Checklist →[67]

These sections of that checklist are especially relevant when it comes to doxxing risks:

- Section 3: Home Safety
- Section 4: Evacuation Planning

☐ Add a security PIN to your bank and cell phone accounts

Your bank accounts and cell phone provider account are high-value targets where you want to add extra protections. Some of these places will only try to verify with your phone number, address, and/or date of birth. All of these are kinds of information someone could find online about you.

Adding a PIN or other security measures helps make sure you are the only person who has access.

HOW TO ADD A PIN TO SENSITIVE ACCOUNTS

Here are some of the accounts you'll want to secure.

1. Bank, credit card, loan, mortgage, and investment accounts
2. Your cell service provider (Verizon, T-Mobile, AT&T, etc.)
3. Internet provider
4. Utility companies
5. Insurance (health, home, auto, etc.)

How to add a PIN for each account:

1. Call their customer service line.
2. Ask if you can add a verification PIN.
3. Generate a random PIN[51] for each account.
4. Save it in your password manager[22].
5. If you can't add a PIN, ask what other security features they offer to prevent someone from pretending to be you and accessing your account.

Tools summary

We link to many tools in this guide and we wanted to capture them in one place:

- Google "Results About You" feature[18]: Notifies you when your personal information appears in a new result on Google.
- EasyOptOuts[4] ($20/year): Removes your info from all the "people search" sites.
- Block Party[20]: Walks you through the exact settings you want to change on each of the most popular social media sites.
- Cyd[23]: Helps you delete/backup your X/Twitter posts (and optionally move them to Bluesky).
- Identity generator from StrongPhrase.net[58]: Helps you have random name/username/etc to put on each site.
- MySudo[32] or Google Voice[31]: Get a secondary phone number so you don't have to share your real number.
- Qwacky to use @duck.com email[63] or Proton Mail[64] or Addy.io[65]: Use an email alias service so you can generate a unique email address on each site that can't be correlated across sites.
- SMSPool[66]: Lets you rent a random phone number for a few minutes to get a verification text when signing up for services that require a phone number.
- Optery[5] ($250/year): For high-threat users. Does the same thing as EasyOptOuts, but goes a little further. (People often suggest DeleteMe, but Optery is more effective.)

Note: Tools only get you so far, some steps have to be done manually.

Responding to doxxing and online harassment

We don't yet have a full doxxing response guide, but we do want to offer some starting points.

Doxxing response:

1. **Prioritize your physical safety:** Go to a friend's house or a safe house if you are worried you might be at risk of imminent harm or harassment. Trust your gut. It's better to lean on support and find out nothing happened than the opposite.
2. **Take care of your emotional wellbeing:** Even supposedly "minor" harassment can be very stressful because you don't know if the threats are going to materialize. Take care of yourself[68].
3. **Get support:** Don't do this alone. Have someone by your side for every step of this.
   - Find friends/comrades who check in with you frequently and help you stay grounded.
   - Reach out to get expert support: Access Now 24/7 Helpline[69] (free), Equality Labs[70], Brightlines[52] (high-end), Convocation Research & Design[53] (high-end).
4. **Document everything:** Don't delete it or block anyone. It can be helpful for tracking down the people behind the attacks later. Delegate this to a supportive person if you need to. How to document[71].
5. **Don't call the cops:** Law enforcement could use an investigation to learn more about activist networks. That said, there might be some situations where local anti-harassment laws could support you. Consider consulting with a movement aligned lawyer before you contact the State and/or bring law enforcement into your situation. Movement-aligned lawyers you might consider: CLDC[72] (rapid response hotline: 541-603-6891) or NLG[73].

Learn more about how to respond:

- Brightlines - Doxxing Resources[74]
- Right To Be - Doxxing Response Guide[75]
- Right To Be - Self-Care guide[68]
- PEN America - What to do if you've been doxxed or placed on a watchlist[76]
- PEN America - Online Harassment Field Manual - Doxxing response[77]
- Crimethinc - Prevention and Aftercare for Those Targeted by Doxxing and Political Harassment[78] (2020)

Keep learning with these related guides

Emergency planning
Establish an emergency support network in case you're detained or threatened.

Signal security
Secure your Signal messaging app for safer communications.

Secondary phone
Set up an extra phone for activism and protests.

Spyware protection
Protect yourself from spyware and surveillance software.

Lockdown Mode trade-offs 2 min read 49 "Police at the door" poster 79

Links

1. theintercept.com/2026/05/13/miami-beach-billboard-truck-david-suarez-israel-gaza/
2. aljazeera.com/amp/news/2025/7/11/canary-mission-how-us-uses-a-hate-group-to-target-palestine-advocates
3. activistchecklist.org/party/
4. easyoptouts.com
5. optery.com
6. fastpeoplesearch.com
7. consumerreports.org/electronics/personal-information/services-that-delete-data-from-people-search-sites-review-a2705843415/
8. innovation.consumerreports.org/wp-content/uploads/2024/08/Data-Defense_-Evaluating-People-Search-Site-Removal-Services-.pdf
9. kanary.com
10. suppression.peopleconnect.us/login
11. nationalpublicdata.com
12. nationalpublicdata.com/optout.html
13. github.com/yaelwrites/Big-Ass-Data-Broker-Opt-Out-List

14. clearview.ai/privacy-and-requests
15. pimeyes.com/en/opt-out-request-form
16. facecheck.id/en/RemoveMyPhotos
17. support.google.com/websearch/answer/12719076?hl=en
18. myactivity.google.com/results-about-you
19. support.google.com/websearch/answer/9673730?hl=en
20. blockpartyapp.com
21. chromewebstore.google.com/detail/block-party-%E2%80%94-deep-clean/hefhjoddehdhdgfjhpnffhopoijdfnak
22. activistchecklist.org/essentials/
23. cyd.social
24. digitalfootprintcheck.com/free-checker
25. kenklippenstein.com/p/ice-making-list-of-anyone-who-films
26. canarymission.org
27. nitter.net/camhigby/status/2015093531526729789
28. theguardian.com/us-news/2025/nov/21/fbi-signal-group-chat-immigration
29. activistchecklist.org/doxxing/
30. signal.org/blog/phone-number-privacy-usernames/
31. workspace.google.com/products/voice/
32. anonyome.com/individuals/mysudo/
33. sideline.com
34. line2.com
35. activistchecklist.org/signal/
36. activistchecklist.org/doxxing
37. bing.com/webmasters/tools/contentremoval
38. google.com/alerts
39. support.google.com/webmasters/answer/7041154?hl=en
40. equifax.com/personal/credit-report-services/credit-freeze
41. experian.com/help/credit-freeze/
42. transunion.com/credit-freeze
43. support.google.com/maps/answer/15439776?hl=en
44. google.com/maps
45. zillow.zendesk.com/hc/en-us/articles/202036344-How-do-I-hide-or-remove-photos-of-my-home
46. support.redfin.com/hc/en-us/articles/360002970072-Upload-Your-Home-s-Photos
47. support.apple.com/en-us/105120
48. landing.google.com/intl/en_us/advancedprotection/
49. activistchecklist.org/lockdown/
50. support.signal.org/hc/en-us/articles/360007059792-Signal-PIN
51. strongphrase.net/passcode
52. brightlin.es
53. convocation.design
54. accessnow.org/help/
55. instantusername.com
56. duckduckgo.com/email/
57. gmail.googleblog.com/2008/03/2-hidden-ways-to-get-more-from-your.html
58. strongphrase.net/identity
59. usps.com/manage/po-boxes.htm
60. ipostal1.com
61. ups.com/us/en/the-ups-store/mailboxes
62. strongphrase.net/username
63. github.com/Lanshuns/Qwacky
64. proton.me/support/pass-email-alias
65. addy.io
66. smspool.net
67. activistchecklist.org/emergency/
68. righttobe.org/guides/self-care-when-experiencing-online-harassment/
69. accessnow.org/resources/
70. equalitylabs.org/services/
71. onlineharassmentfieldmanual.pen.org/documenting-online-harassment/
72. cldc.org
73. nlg.org
74. brightlin.es/anti-doxxing-resources
75. righttobe.org/guides/responding-to-online-harassment/
76. pen.org/online-abuse-digital-safety/what-to-do-if-youve-been-doxed-or-placed-on-a-watchlist/
77. onlineharassmentfieldmanual.pen.org/respond/
78. crimethinc.com/2020/08/26/doxcare-prevention-and-aftercare-for-those-targeted-by-doxxing-and-political-harassment
79. activistchecklist.org/police/