EQUALITY LABS

ANTI-DOXING GUIDE FOR ACTIVISTS

Publication Notice

This is an *advance copy* of our anti-doxing guide. Please refer to Publications and Resources to access the latest version of this guide.

Information in this document may be deprecated at time of reading. Please check our Digital Security page on our website for continuing updates to our digital security guidance.

Follow us on our socials to know when we release updates to this guide.

twitter.com/equalitylabs

instagram.com/equalitylabs

Publication Notice:
This guide has been prepared for advanced release on Monday, October 16, 2023.

This is an advance copy of our anti-doxxing guide. Please check this link on our website for continuing updates.

Information on this document may be deprecated at time of reading. Please refer to this link to access the up-to-date version of this guide.

Introduction

Equality Labs is a Dalit-led, feminist, digital security, technology, and political organizing startup dedicated to progressive power-building. We provide practical tools for communities to intervene and disrupt longstanding systems of oppression and to advocate for themselves. You can learn more about us by visiting our website.

Since publishing our first anti-doxing guide in 2017, the practice of doxing has evolved dramatically. Our team wanted to revisit this topic and give our communities the opportunity to take digital security into their own hands. We hope that this guide will encourage and prepare you to build a comprehensive safety plan within your communities. Whereas the original 2017 anti-doxing guide explained how best to secure your digital identity after being doxed, this iteration offers proactive security measures and best practices to adopt before becoming the target of a doxing campaign. As always, all security work should be non-reactive; we encourage readers to anticipate incidents and prepare for the future.

We have created this anti-doxing guide to support activists around the world who may be targeted for resisting white supremacy, Islamophobia, casteism, antisemitism, anti-LGBTQ+ harassment, or any form of authoritarianism.

We know that the escalated activities of white supremacists and Hindu nationalists are frightening, but the best defense remains rooted in information, awareness, compassion, self-care for ourselves, and community care for each other, plus a commitment to collective resilience.

If you have any questions, contact us on Instagram, Twitter, or Facebook.

This guide may feel overwhelming and the information hard to digest. Acknowledging that we want to focus on building our collective capacity along with a sense of safety and security, we encourage folks to reach out to us at any time with any questions or concerns. We offer consultations ranging from individual rapid response cases to organizational security operations and audits.

What is Doxing

Doxing is the internet-based practice of researching, documenting, and broadcasting PII (private or personal identifiable information) about an individual or organization to harass and traumatize activists. Additionally, such attacks can also be accompanied by physical violence, intimidation, psychological harassment, weaponized unreality, and disinformation about an individual and/or a movement—all of which have serious implications for our livelihoods and safety.

The term “doxing” comes from the word “documents.” 1990s hacker culture shortened the term to “docs” and then “dox,” with “dropping dox” referring to finding personal documents or data (like someone’s physical address) and publishing them online.

We believe that many of the far-right and Hindu nationalists are using the social media ecosystem to harass activists and spread disinformation. Bad actors can acquire your personal information by searching publicly available databases like data brokers and social media websites like Facebook, LinkedIn, and Twitter as well as through hacking and social engineering.

Have You Been Doxed?

Today, doxing is unfortunately more popular than ever, with many unsuspecting individuals and organizations finding their information posted on high-profile platforms such as cable news, large social media accounts, image boards, or online forums. Being mentioned on a large platform isn't inherently a dox but can lead to targeted harassment. So how do you know if you've been doxed?

If you've seen someone post your name, address, phone number, email, picture, or other contact info publicly on social media or a forum, you may have been doxed. If you're suddenly getting an influx of emails, phone calls, and text messages to your home or workplace but haven't seen your information posted anywhere, you've likely been doxed somewhere.

Every sudden influx of negative messages is not necessarily due to a dox. When just one person appears to be harassing you, you may be the victim of an online harassment campaign, a cyber-bully, or a stalker. If you have been the victim of domestic abuse and/or feel that you may have a stalker, check out the Additional Resources for this section.

Additional Resources:

- DIY Cybersecurity for Domestic Violence
- Resources-Survivors — Safety Net Project
- Guide to Abortion Privacy — Digital Defense Fund

Common Signs You've Been Doxed:

- A sudden influx of harassing phone calls, text messages, emails, physical mail, or social media comments, often from people you do not know.
- People showing up to your home or workplace asking specific questions about you or referencing your political beliefs or online activity.

If any of the above has already happened to you, you should take immediate steps to protect yourself.

Things That May Feel Like Doxing, But Are Not:

- Someone mentioning your name or username on social media.
- Many people sharing/retweeting a post you made while making negative comments about you.
- Being mentioned in a news article or blog post.
- A large account sharing your posts, footage of you, or discussing you in an attempt to attract unwanted negative attention towards you.

Create a Self-Care Plan

Seek Support From Your Communities:

One of the most crucial yet overlooked steps you can take is to recruit friends and family to support you. Let your network of support know what's going on. Online harassment is traumatic, and you must prioritize your mental and physical health so that you can work through these attacks. Informing those closest to you about what you're experiencing allows them to help them help you.

Talk to members of any communities you may be a part of. Let them know what's going on and how you need support. Examples of support can include checking in regularly, visiting, dropping off food and supplies, running errands with you, staying over at your home, helping scrub your data off the web, helping report accounts targeting you, helping secure your home, and going through the steps of this guide together.

Do not limit this to just your activist communities. Talk to your family if you are comfortable doing so. CrimethInc's Doxcare guide has a great section on how to have these difficult conversations under the "Having Conversations with Jobs and Family" section. You should also consider having these conversations with neighbors as well. Encourage them not to ignore strange or loud noises indicating something may be wrong. Ask them to check on you if they notice something suspicious. Your communities are your biggest asset and the best line of defense against attacks from right-wing extremists.

Some Examples of Support Include:

- Asking someone you trust to check your emails, social media, and other accounts for you.
- Asking someone to keep an incident log of the harassment, including where it originates (if known). *More on creating an incident log below*.
- Asking someone who works with you to back you up should trolls contact you or show up to your workplace.
- Asking someone to check on you often during the harassment and make sure you're okay.
- Asking someone to provide you with a safe place to stay if the situation escalates or if your home address is shared.

Share this and other guides with friends and allies so they can understand what's going on. Be specific about what's happening and the support you need. Share with people:

- That you are at risk of being targeted.
- How that affects you, and how it can affect them.
- What they need to do to minimize the harm.
- How they can best support you.

Encourage friends/family to complete some of the anti-doxing steps. For example:

★ "Hey here's a thing that might be happening now or soon, because of my work, please take these steps to protect me; also be aware that this might be happening to others who work on this, and here are things you should be aware of and other groups you should be contacting."

We take our lead from our collaborators at Stop LAPD Spying Coalition, Lucy Parsons Labs, CryptoHarlem, Vision Change Win, Hacking//Hustling, and Electronic Frontier Foundation who talk about adopting a vision of security culture that centers collective security practices as an expression of love and solidarity. As activists, we know the power of compassion. When we look out for one another we access a greater capacity than we

could manage alone. By tapping into our relationships, we make ourselves more difficult targets for bad actors.

Thus, even when you are under attack, give space to your feelings of anxiety and dread, but do not succumb to them. Release them and assert your agency. In these situations, we can adopt a culture of mutual aid and support around digital security. We can build power instead of paranoia. We can create a community of practice that normalizes multiple ways of knowing and creates new patterns of behavior.

Security Planning and Threat Models

What is a Threat Model?

Creating a threat model may sound complicated, but it can be a relatively simple way for you to ground yourself and take the most appropriate precautions given your situation. Threat modeling is a practice in which you carefully assess the likelihood of an adverse event, weigh that likelihood against the potential impact of that event, then use those two factors to determine which security measures you should prioritize and which you should ignore. This process is best done with a trusted friend, family member, or security practitioner. Threat modeling can help you ground your fears in reality by helping you to assess which threats are the most likely to occur. If you are not sure about how likely certain threats are, it's best to threat model with a trusted friend or security professional.

Not all of the information in this guide may be relevant to you. Threat modeling can help you determine which steps to prioritize in this guide, which steps to ignore, and even how to plan for threats outside the scope of this guide. Your threat model may vary depending on who you are, what demographics you belong to, who is targeting you, where and when your information was posted, where you live, and many other factors. By identifying your most vulnerable or likely threats, you can take action to prevent or disrupt surveillance.

Below we expand on the Electronic Frontier Foundation's advice from their Surveillance Self-Defense series. We encourage you to use these prompts as you create a threat model and begin developing a security plan that works for you.

Factors to Consider When Threat Modeling:

- **Do you have realistic goals or expectations?**
    - Examples of realistic goals:
        - Wanting to scrub your personal data from websites.
        - Locking down your social media.
        - Improving your home/work security.
    - Examples of unrealistic goals:
        - Becoming untraceable or going off-grid.
        - Being undoxable.
        - Making your house impenetrable.
- **Keep an incident log of attacks or harassment you're experiencing**
    - Analyze what people are saying about you and the frequency of these attacks. Use this data to come up with a list of immediate steps to take.
        - If people call your home threatening to burn it down, you may want to stay somewhere else for a while or set up some home security.
        - If people are talking about showing up to your workplace, ask your employer about working from home or taking time off if possible.
        - If people are threatening to show up to your next drag performance, notify the venue and work with them to make a plan. A plan can consist of beefing up your own and the venue's security, mobilizing the community to protect each other, or even canceling your performance.
    - Keep track of the who, what, where, why, and when: Who posted information about you? What did they post? Where did they post it? When did they post? How can the answers to these questions inform your threat model in defining what you are most at risk for?

- **What information are you most concerned about or is most vulnerable? What are the consequences?**
    - Are you concerned that someone will find out (or already has) your personally identifiable information (PII) such as your home address, phone number, or details about your workplace?
        - If this is a primary concern, skip to this part of the guide, which explains how to identify and remove publicly available information on you.
    - How and where is your information stored? Physical device? Transmitted online? The cloud?
- **Who are you concerned about: an individual or "civilian" group, a corporate or government entity?**
    - Who is targeting you: law enforcement? A corporation? A stalker? Far-right extremists?
    - What information do they want? Are they targeting you alone or are they targeting communities and groups you belong to?
    - Remember that non-state affiliated individuals will typically have less sophisticated methods than the state or law enforcement. Knowing who is targeting you will help you decide which steps to take immediately.
- **How might you be surveilled?**
    - If a state-affiliated actor is targeting you, you may want to prioritize removing yourself from some databases known to be used by law enforcement such as Palantir, CLEAR, LexisNexis, and ClearviewAI. It is unrealistic, however, to expect to remove yourself from every data source available to law enforcement. We also want to note that removing yourself from a database such as LexisNexis can have impacts on getting background checks for work or for housing, insurance, and possibly finance.

- **Assess your risk: How serious are the consequences?**
    - Know that there is an important difference between possibility and probability when designing your threat model.
        - It's possible you can be monitored by police 24/7/365, but very improbable. If you simply attended a protest without incident, law enforcement is highly unlikely to use costly and sophisticated resources to monitor you intensively. There is of course a middle ground here; everything depends on your particular situation. Ask yourself if the cost of surveilling you would truly benefit law enforcement.
            - If you are still not sure about the capabilities of the state, visit the State Surveillance section of this guide where we try to demystify when, why, and how state surveillance is used.
    - If your personal identifiable information has already been posted online, you are at greater risk. You should follow steps in this guide to remove and secure your online information.
    - Prioritize the risks that you will take most seriously over ones that are harmless, rare, or too difficult.
- **Pick what works for you: There is no one-size-fits-all security plan or threat model.**
    - Not everyone needs to follow every step in this guide, and some will need to seek resources outside the scope of this guide. This section should help you prioritize which steps to take first.
        - For example, if people are simply threatening to find your information online but haven't posted anything yet, you should quickly scrub as much personal information off the web as you can and lock down your socials. On the other hand, if someone already has posted information on you and several people are talking about burning your house down, you should vacate your home and stay somewhere safe if possible, notify your friends, family, and coworkers, then take other steps in this guide as needed.

- How much work are you able to do before or after being doxed? Handling your security before or after a dox can be stressful, taxing, and traumatizing. Lean on your support networks and tap into your self-care contingencies. You do not have to go through everything alone. We are much harder to target by both state and non-state actors when we have built robust communities of trust.

- The more energy you and your communities devote to protecting each other, the more difficult it will be to target you.

Common Threats and Their Likelihoods

In most instances, doxing is a tactic designed to put you in a state of fear and panic. It is a violation of your privacy, and safety that can lead to lifelong trauma and fear, but most cases of doxing do not lead to physical harm. (This is not to say that physical harm cannot occur as a result of doxing.) Below we list some common threats that may become more likely following a dox. The likelihood of any of these occurring depend on your unique situation.

If you would like more guidance in assessing and remediating threats as a result of a dox or a harassment campaign, reach out to us at any time with any questions or concerns. We offer consultations ranging from individual rapid response plans to organizational security operations and audits. Please reach out here: inquiries@equalitylabs.org

Harassing Communications (phone calls, emails, physical mail)

Following a dox, attackers will look for the easiest way to harass you. Beyond reposting a dox itself, the lowest-hanging fruit for them is to harass you via phone calls, emails, text messages, DMs, or sometimes physical mail. These messages can be extremely distressing to view. If you can, ask a friend to screen these messages for you.

Sometimes these messages take the form of violent threats that can indicate an increased likelihood of a physical incident. These can include someone sending you a unique photo of the outside of your home (meaning they likely took it themselves and did not get it online); a single person repeating the same extremely violent threats towards you and indicating their intention of carrying them out; a suspicious person or vehicle

suddenly appearing nearby following a dox; or someone showing up at your home. All these may be considered an escalation in tactics and appropriate precautions should be taken.

Attacking Your Accounts

Reporting social media accounts, spamming your comments sections and DMs, creating accounts impersonating you, trying to hack into your accounts and financial institutions, searching for abandoned accounts to find information, and digging through your old posts are common harassment tactics used against people who have recently been doxed. Our guide will walk you through the steps to reduce the impact of these particular threats. See:

Find out what information trolls can find about you

Change all your existing passwords

Turn on 2-factor authentication

Protect your financial life

Create a self-care plan

Contacting or Harassing Loved Ones

It's just as easy for harassers to find information about your loved ones as it is to find information about you. Depending on your situation, those closest to you may receive harassing or concerning messages as a result of your dox. These messages may include nasty comments or rumors about you, fake images of you, or even phishing attacks.

In some instances, you may wish to engage those closest to you regarding the harassment you're receiving. Having conversations about a dox with your loved ones may be complicated. CrimethInc's Doxcare guide has excellent advice on this matter under their "Having Conversations with Jobs and Family" section. Beyond having these conversations, you may wish to encourage those around you to improve their security practices by referring them to this guide.

Contacting Your Workplace

Attackers may find your workplace through a data broker, your LinkedIn profile, posts on your social media, or some other means. If your workplace is advertised in a dox, your employer may receive emails and calls spreading nasty rumors or disinformation about you in an attempt to have you fired.

Depending on your relationship with your employer, you may wish to preempt a potential harassment campaign by discussing the situation with them while being careful not to give them unnecessary details. Your employer may assume you did something wrong. One tactic when this happens is to steer the conversation away from yourself and to the nature, tactics, and goals of your attackers. If you are lucky to be a part of a good union, you may wish to have a union rep present in the room as an advocate. If you are not part of a union, see if you can leverage your workplace relationships into a network of support. CrimethInc's Doxcare guide has further excellent advice on this matter under their "Having Conversations with Jobs and Family" section. They also link to this helpful 1-pager by Crash Override Network, which you may wish to print out and share with your coworkers and employer.

Some attackers may call your workplace posing to be a friend or loved one to gain personal information about you, such as the hours and days you are present in the workplace. It is important that neither your coworkers nor bosses share personal details with anyone outside the workplace.

Stalking

Although typically employed against women, stalking is not gender specific. While incidents of stalking are not bound by circumstance, many victims of stalking tend to be content creators. You might notice a single user becoming increasingly invasive, aggressive, and obsessive. This user may also utilize several different accounts to harass you. Stalking can happen independently of a dox. Sometimes a stalker will use the same methods as doxers to find information about you. Sometimes they will disclose this information publicly to intimidate you or try to make you give in to their demands.

Stalkers may comb through your online posts to find clues as to your whereabouts. They might analyze the background of your photos to identify the layout of your home, look for landmarks to help narrow down your location, note the make and model of your vehicle, and create a map of which restaurants or other locations you have visited.

If you find yourself at an elevated risk of stalking, we encourage you to archive or delete old posts. (Understand that an adversary may have already saved copies of this content.) Be wary when uploading images or videos with backgrounds that may have identifiable elements. We recommend turning off your location settings across your social media. If you must tag a location, do so in a post made several days after you have left that area.

Swatting

A swat attack or "swatting" is when an attacker takes advantage of a militarized and violent police force by placing a false emergency call, often posing to be you, to provoke law enforcement to go to your home, workplace, or school where they expect a deadly encounter. The attacker will make it seem as though you are engaged in a life-or-death situation and that you are a danger to law enforcement. This can result in a highly militarized team of law enforcement surrounding your home, breaking down your door, pointing weapons at you and whoever else is in the home, and sometimes death or severe injury. Swatting is perhaps the most dangerous consequence of doxing. It is also the least likely. While swatting does not often lead to death or physical injury, it can result in lifelong trauma and fear.

Who is most at risk for swatting?

Your personal risk for swatting depends on your situation. Streamers, public figures, gamers, online content creators, activists, or marginalized people who have just been doxed are at a heightened risk of swatting. Your risk of swatting can potentially increase based on how high profile you are, what communities you belong to, if you are being targeted by a campaign, if you are featured in the news, or if a high profile individual or outlet repeatedly makes concerning content about you designed to elicit outrage.

Signs of a Potential Swatting Attack

Getting calls to your home, threats of swatting you, or strange deliveries to your home are often signs of an imminent swatting attack. These tactics are, however, more likely used in isolation and do not escalate to a swatting attempt; even so, you should begin to take precautions. Consider notifying your friends and family or staying somewhere other than your home for a while, if possible.

How you can reduce your chances of being swatted

Everyone can reduce their chances of getting swatted. The most important preventative measure you can take is to avoid divulging personal information online. This includes your real name, general location, contact information, and anything else that can be used to narrow down where you live. You can also take steps to remove your information online by skipping to this portion of the guide. It is more difficult for an attacker to swat you when they don't know much about you. We recognize this can be difficult for content creators who make their living posting online, but there are still things you can do.

Do not share your phone number or email address. If you must have a phone number or email to give out to people, make them specifically for that purpose and do not use them for any other reason. Be wary when posting footage or images of the interior or exterior of your home, as attackers can easily locate you using this material. Make sure any images you upload or send to others do not contain your location information stored in metadata. If you are a content creator or a gamer, try to avoid using the same username across social networks or games. Often, aliases such as gamertags are reused across services, which can make it much easier for someone to find information about you. Following the steps in this guide will also help reduce your chances of being doxed.

Should I Involve Law Enforcement?

Risks of Involving Law Enforcement

There are always risks when dealing with law enforcement, especially for activists, those who are marginalized, formerly incarcerated, and human rights defenders. Sometimes law enforcement themselves engage in dox-like behavior. Members of law enforcement may also be part of the same groups as your attackers. CrimethInc's Doxcare guide wisely mentions that if you are part of an activist group, law enforcement may even use your reaching out to them as a way to gain more information about you and your circles rather than protect you in any meaningful way. Even if you trust law enforcement, there is often very little they can do in the event of a dox unless much more severe and violent crimes have already taken place.

In the event of a dox, trust your communities to protect you: your neighbors, your activist circles, your friends, your families, and possibly even your employers. Involving law enforcement is an extremely personal decision. If you still choose to involve them, it is your responsibility to disclose their involvement to anyone who may be at risk.

Reducing Encounters with Law Enforcement

If you suspect you may be targeted with theft, burglary, or other activities which may cause harm to you and you wish to create a trail of evidence for insurance or legal purposes, many law enforcement agencies will allow you to create a police report online without having to encounter an officer or provide specific information that may be of interest to law enforcement. Most police reports do not receive any follow-up from a member of law enforcement. If you choose to do this, you may wish to use a unique email address and phone number created for only this purpose.

Be aware that submitting a police report may supply law enforcement with information. In some cases, especially if you are already on the radar of law enforcement, filling out a police report can result in unwanted police attention focused on you, members of your household, or your activist circles. Folks on probation or anti-police activists may be at greater risk.

Additional Resources:

- Security Planner | Consumer Reports
- CrimethInc.: Seven Myths about the Police
- CrimethInc.: What Is Security Culture?
- CrimethInc.: Doxcare: Prevention and Aftercare for Those Targeted by Doxxing and Political Harassment
- Our Enemies in Blue

Create an Incident Log

Creating an incident log will reveal patterns of attacks and, when your log is compared with those of other organizers, surface even larger patterns. This information can help you identify opponents and their organizations.

A sample log might look like this:

INCIDENT RESPONSE LOG

DATE	TIME	DESCRIPTION	RESULT/RECOMMENDATION

Keep notes throughout your attack to share with a security professional and members of your team. If you like this example, you can make a copy.

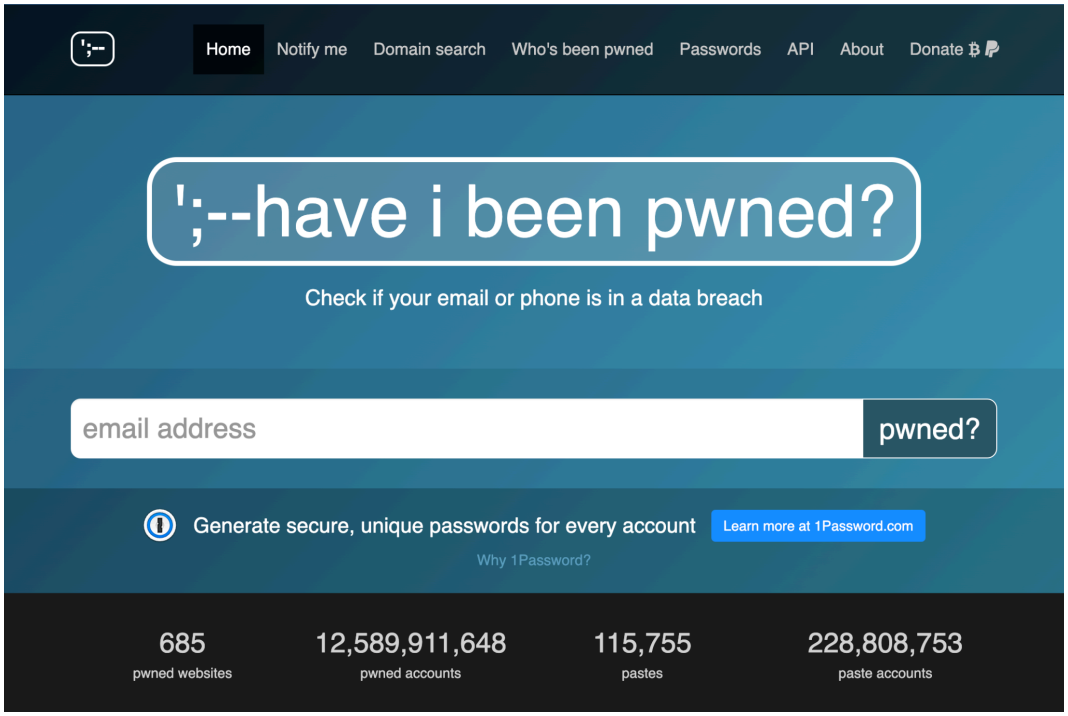
Please note: We recommend that you keep incident logs using an encrypted and password protected word processing platform like Etherpad on Riseup or Cryptpad.

Protect Your Passwords/Passphrase

Change All Existing Passwords/Passphrases

Chances are you've been using the same email addresses and passwords for years. A quick search of your email addresses on the service HaveIBeenPwned can reveal if and when your email address and other sensitive information were part of a data breach. These breaches allow any troll to access your personal information, including your full name, email addresses, passwords, Social Security number, and more. We strongly recommend every use of a passphrase, rather than password, that is at least 18-24+ characters in length, best practices have changed, and numbers/special characters/capitalization are no longer recommended as people tend to choose weaker passphrases in order to accommodate these criteria.

One crucial step to take when you've been doxed or subject to a harassment campaign is to change all your passwords immediately. This may sound daunting, but begin with your most commonly used or most sensitive accounts, such as your financial institution and primary email addresses. You should then revisit HaveIBeenPwned and prioritize your compromised accounts.



After that quick assessment, make a list of all of your crucial accounts and change the passwords immediately so you have fresh passwords/passphrases for each. You can test the strength of your passwords here. We strongly recommend "passphrases" rather than passwords—the longer the better, with numbers, symbols, and special characters too. Your passphrase should be **unique** to each platform or website.

We strongly recommend incorporating a password manager to generate and store all of your new passwords. This will allow you greater capability to create complex, unique, randomly generated passwords for all of your accounts, while only knowing one password for your password manager. We recommend 1Password or Bitwarden. While it may be convenient, we strongly recommend *against* using your internet browser (e.g., Firefox, Chrome, or Safari) to store your passwords. We also recommend turning off password management in your browser so that you do not receive prompts to save your passwords. Attackers know where these passwords are stored and how to obtain them. Many reputable password managers have browser integration, which is a much safer method to store your passwords and use autofill.

If a digital password manager feels too complicated, you need to access passwords offline, or you are not confident in your tech skills and would like an analog approach, we recommend storing passwords in a nondescript notebook that can be kept in a safe place. Writing down passwords makes them physically vulnerable as they can be stolen, but not digitally vulnerable since they cannot be hacked. No matter what solution you

choose, each password (or preferably passphrase) should remain unique to each login. Do not reuse passwords across logins.

Best Practices for Passwords

A good password should be 18-24 characters in length and should ideally include a mixture of uppercase and lowercase letters and numbers while a good passphrase should contain at least 6-8 randomly generated words separated with a space. The more you add to a password, the stronger it can be. The most important thing about your password is that it should be impossible to guess but still simple enough for you to memorize. Hopefully you should only have to memorize only a few passwords including the passwords to unlock your phone, computer, and your password manager. Incorporating a password manager in your digital life should dramatically reduce the amount of passwords you need to memorize, help you organize all your accounts, and allow you to generate long, complex, and secure passwords.

Good Passwords vs Bad Passwords

Good passwords are extremely difficult for either a human being or machine to guess.

Bad passwords are ones that have been used before, are small, and contain common names, phrases, or dates.

For example, the passwords "humptydumptysatonawall" or "HumPTyDumptY$@t0n@waLl" can be easily cracked by a machine, whereas passwords such as "Fm9DCCThh4u9cdSsEu" or a passphrase containing random words such as "Unfunded Gaining Proofread Bloating Fanfare Anything" can take years, even centuries for a computer to crack. Please do not use any of these passwords as they are just examples and not secure to use since this is a publicly available document. These are examples of the types of passwords you can generate using a password manager. We strongly encourage you to keep generating random passwords until you find one that you feel comfortable memorizing. It is also okay to write passwords down somewhere safe (not on a sticky note posted on your device) until you have memorized them. If you feel like you cannot memorize a randomly generated password, it's okay! Do your best to come up with something that follows this advice and appears as impossible to guess gibberish.

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

The image above is from Hive Systems © 2023: Are Your Passwords in the Green?

Additional Resources:

- Data Breach Guide — Digital Defense Fund
- Account Security: Passwords & 2FA Slide Deck — Digital Defense Fund

Turn on 2-Factor Authentication (2FA)

Turning on 2FA can thwart the majority of malicious attempts to gain access to your accounts. 2FA requires more than just your password to log in to your accounts. Usually

2FA takes the form of a randomly generated one-time code generated through an authenticator app or sent to your phone via SMS. Using 2FA ensures that even if a bad actor knows your password, a randomly generated code is sent to you, not your attacker.

When deciding which accounts should feature 2FA, think like a troll. Which accounts do you have that would cause the most damage if they were compromised? By taking over your email, someone can release and interfere with your communication; by taking over your bank account, an attacker can wreak havoc with your finances. Ultimately, we recommend you **lock down all your accounts.**

2FA is available for services such as Gmail, Facebook, Twitter, Instagram, Amazon, and more. When possible, avoid using text/SMS as your method of verification. Texts can be intercepted, making it the least secure option for 2FA, especially if your adversaries are technologically capable. We recommend the app Authy or Google Authenticator to generate and store your 2FA codes. This app can generate codes on your phone and can be revoked remotely if your phone is confiscated, stolen, or lost.

Activating 2FA can be a time-intensive effort, and we recommend you prioritize your mission-critical accounts first. Please check out our Passwords/2FA checklist example for an idea of what kind of accounts might be relevant to you.

Mission-critical accounts might be

- Financial accounts (banks, payment platforms, work HR platforms, investment platforms)
- Accounts tied to your location and legal ID (utilities, governmental agencies).
- Social media accounts (social media platforms, dating services, professional networking platforms, event management platforms).
- Core services (high-traffic services used in your daily life, core work tools and platforms, educational platforms, entertainment platforms).

Discover What Information Trolls Can Find About You

The best way to see what information trolls can find out about you is to search for yourself using a search engine like Google, Bing, and DuckDuckGo. You will get a sense of how much data exists about you online. A search also gives you a starting point to try and take down as much of your information as possible. After that initial search, you can go on to examine all the data broker sites that trade on personal information. From here, you have two options:

Option 1: Use paid data scrubbing services such as DeleteMe* or Privacy Pros* to remove information. This approach is best if you are overwhelmed by the process, cannot do it yourself, or are pressed for time. Here's a video review of their service and how it works. Even if you go through this service, there are still steps you should manually take to scrub your data.

*Note that these paid services can sometimes take weeks or months to get information removed.

Option 2: DIY. After searching yourself online, opt out of the most prominent results that share your information and use a guide to scrub your data off other data broker websites. Our co-collaborator Yael Grauer has produced a comprehensive and often updated list of current data broker opt-out processes: yaelwrites/Big-Ass-Data-Broker-Opt-Out-List.

Although it is difficult to scrub all data about you online, removing what you can makes it harder for an adversary to target you. In response to an urgent case of doxing and if you are simply over capacity in terms of your rapid response capabilities, consider using a service like DeleteMe. They have been working with activists around the country to scrub their data.

In some cases, you can get Google to remove data about you. If you see personally identifiable information, you can remove it via this tool.

If you see your data posted on major platforms like Twitter, Instagram, Facebook, or even spaces like 4chan, then be sure to report the post if possible. (**Note:** Take caution when visiting websites like 4chan. You will be exposed to disturbing content and your IP may be logged. For more info, read our section on VPNs.)

In some cases, you may find your personal information listed on a government form (e.g., a campaign donation record, city hall transcript, or even voter registration record in some states). In these cases, call the website owner or the agency and explain that you are the victim of harassment and need the records redacted. Agencies will usually comply. Be sure to be polite and emphasize the harms you're experiencing as a result of having this information publicly available.

Facial recognition can be used to target people. Two platforms worth opting out of include Pimeyes and Google Images.

Finally, if you are a resident of a state with Data Protection laws like the CCPA in California, CPA in Colorado, or PIPA in Illinois, you have the right to request deletion of your data from any business. Connecticut, Utah, and Virginia have new data protection laws as of 2023. These US privacy acts are based on the European Union's GDPR (General Data Protection Regulation). In many cases, you are not required to submit proof that you live in these jurisdictions, meaning companies will usually honor these requests regardless of residency. For more information, look through the company's Privacy Policy and search (usually Ctrl+F or Command+F) for your state's name in quotation marks.

Protect Your Financial Life

Trolls will often escalate online attacks by trying to go after your credit cards, utilities, and bank accounts. Call your financial institutions, utilities provider, and any other major service provider to let them know you are a target and they will typically add an additional layer of security that can help protect you. If you haven't already, be sure to change your passwords to these services and utilize 2FA or multi-factor authentication if available.

If you suspect attackers may go after your financial accounts or credit, you may want to consider instituting a credit freeze. A freeze prevents would-be attackers from stealing your identity and using it to take out loans, open new credit cards, or make other major changes to your financial life.

While a credit freeze will stop a bad actor from opening a new line of credit, it will also stop *you* from opening new financial accounts, lines of credit, taking out loans, or

undergoing financial background checks. You can always lift a credit freeze, but keep all this in mind if you apply for a credit card or loan, so you won't be rejected due to your credit freeze.

Below are some credit best practices (US-specific):

- Pull your credit reports (annualcreditreport.com) and make sure they are correct.
- Freeze your credit with the big three, so no new lines of credit can be opened. This will prevent almost all attempts to steal an identity.
    - Experian, TransUnion, and Equifax (The Big Three)
    - **Note:** There are smaller credit bureaus, and you can technically freeze your credit with them as well, but it often has more ripple effects (like a landlord not being able to pull a credit report). Should you go that route they are Innovis, ChexSystems, LexisNexis, MicroBilt Connect, and NCTUNE.
- A credit freeze blocks people from opening new lines of credit in your name, but it's not foolproof. If you want another layer of security, also implement a fraud alert (free) with the big three.
    - **Why?** A credit freeze can often be lifted with commonly found PII. A fraud alert in place will force the vendor to verify additional information before lifting a freeze, usually through a phone call to the verified phone number attached to the fraud alert (as well as potentially other approved numbers). This is an extreme scenario though, and any measure of security in locking down your credit will help exponentially.
    - **Note:** Fraud alerts can also be implemented on their own to add additional friction between bad actors and your information, should a credit freeze feel like too much.

Additional Resources:

- Security Planner | Consumer Reports
- IdentityTheft.gov
- What To Know About Credit Freezes and Fraud Alerts | Consumer Advice
- Fraud Alerts & Credit Freezes: What's the Difference?

- Your Online Account | Internal Revenue Service

Install a Virtual Private Network (VPN)

A VPN is a mechanism that acts as a secure tunnel between your device and the internet by encrypting and routing all of your web traffic through the VPN's services. Thus your Internet Service Provider (ISP) cannot view your web traffic. A VPN also assigns you a new publicly facing IP address as opposed to the one assigned to you by your internet service provider, which can allow you to privatize your network traffic and bypass filtering happening at your internet service provider (ISP). It also makes sure that trolls can't find you using your IP address. The latter is especially important as IP addresses have some geolocational information that can be intercepted.

WITH A VPN

WITHOUT A VPN

We recommend VyprVPN, Mullvad, ProtonVPN (which is free), and TunnelBear. Be sure to **always read the privacy policy** to make sure your service does not sell, store, or share your data, and that they will protect it if engaged by the state. There are several common

VPNs out there that you may recognize. We still recommend going through the privacy policies, as there have been many instances of VPNs caught in compromising scandals.

Many advertisements for VPN services tend to be misleading about how exactly a VPN can protect you. While there are many ways they can protect you, using a VPN will not hide all your online activity. In the case of doxing, masking your IP address and encrypting your web traffic through a VPN can simply make it more difficult for harassers to find information on you. For a thorough, easily understood resource that details exactly how a VPN can and cannot help you, read this article by Yael Grauer in *Consumer Reports*.

Additional Resources:

- Should You Use a VPN? - Consumer Reports
- DDF Guide to VPNs — Digital Defense Fund

Protect Your Web Browser

For most people worried about their privacy or security, switching to a browser such as Firefox and using the uBlock Origin, Privacy Badger, and Firefox Multi-Account Containers add-ons plus switching your default search engine to DuckDuckGo can go a long way in reducing online tracking. If you'd like more options, we recommend using Firefox, Brave, DuckDuckGo for Mac (beta), or Mullvad for browsers on your desktop with the uBlock Origin and Privacy Badger add-ons. For Firefox we recommend using the Firefox Multi-Account Containers and Facebook Container add-ons and using them to compartmentalize your browsing. On mobile, we recommend Firefox Focus, DuckDuckGo, or Brave for your browsing needs. Whether on your phone or your computer, we strongly recommend changing your default search engine to DuckDuckGo. We also recommend utilizing Incognito or InPrivate browsing for some sensitive tasks—though only after reading up on how it works. For more sensitive browsing needs we suggest you read our sections on VPNs and Tor.

Chances are you are currently reading this guide on a web browser, such as Google Chrome, Mozilla Firefox, or Safari. Web browsers are probably our most frequently used portal to the internet. This makes your web browser an easy way for information to be gathered about you by advertisers and other online services.

Our browsers can expose a massive amount of personal information to the internet. Almost any website can obtain your IP address and operating system along with what hardware you use, information about your ISP, what extensions or add-ons you use, and much more. This information is primarily useful to advertisers who try to build a dossier or "fingerprint" of your unique web activity. In limited though increasingly common circumstances, this type of information can also be made available for purchase, and bad actors may use it to target activists or marginalized groups. Another way your browser may be unsafe is if you may have unknowingly installed malicious browser extensions.

The “Additional Resources” below contains tools for you to assess what your browser reveals about you, as well as how these processes work. In this guide, we are primarily concerned with individuals whose threat models may involve having this data used against them by a sophisticated bad actor, troll, or law enforcement. Much of the advice in this section is also useful for those who wish to take simple steps to reclaim their online privacy.

Here are some ways you can better secure your web browser:

For web browsers on your computer, we recommend Firefox, Brave, DuckDuckGo for Mac (beta), or Mullvad. For your phone, we recommend Firefox Focus, DuckDuckGo, or Brave. We also recommend switching your default search engine to DuckDuckGo. If you currently use a different browser such as Google Chrome, Microsoft Edge, or Safari, we are not necessarily asking you to switch all your browsing activity from one browser to another. This is a personal choice that depends on your threat level and what level of privacy you would like to achieve. **For most people worried about their privacy or security, switching to a browser such as Firefox and using the uBlock Origin, Privacy Badger, and Firefox Multi-Account Containers add-ons and switching your default search engine to DuckDuckGo can go a long way in reducing online tracking**. We also recommend periodically deleting your browsing history, cookies, and cache if you can. The Firefox Multi-Account Containers add-on gives you the option to partially compartmentalize how you browse the web. Each container acts as a silo, separating browsing history and cookies from all other containers. This allows you to assign separate containers for different purposes and can therefore help reduce tracking through cookies. For individuals with a higher threat level, this may help but not be enough. While these methods aren't perfect and can't make you untraceable, they can help you reduce tracking online.

Reduce Browser Fingerprinting

While the strategies listed above are meant to reduce (**note:** not eliminate) tracking via cookies and your IP address, there's still the issue of tracking via your browser's fingerprint. There is no simple and easy way to completely or even significantly reduce being tracked via your browser fingerprint. Your device hardware, operating system, system and browser settings, IP address, and many other factors can be used to identify your browsing habits.

One of the simplest strategies we have to reduce fingerprinting is using a pre-configured browser, such as the Tor or Mullvad web browsers. Both browsers, when used properly, are designed to have the same or a similar fingerprint between anyone who uses them. This can make it more difficult for trackers to find unique characteristics to associate with you. For more information on how and when you should use Tor, visit our Tor Browser Considerations section below.

The Mullvad browser is best used in conjunction with a VPN and with default settings intact. It offers more robust access and functionality to the web as opposed to Tor, since using Tor can be slow and many online services blacklist connections associated with the Tor network. Like Tor, using the Mullvad browser alone is not enough to make you "anonymous" on the web. By default, Mullvad deletes all your browsing history, cookies, and most of your cache upon exit. This can partially help separate your web activity between sessions. If you wish to more fully separate your web activity, you should use a different VPN connection each time you use the browser, and preferably between different browsing tasks.

Takeaways

While techniques like this are some of our best defenses against browser fingerprinting, they may not be sufficient enough to prevent all tracking. If you've made it this far and feel like you have a handle on things, feel free to skip ahead. If you read the above and still have some questions, this next section is for you.

This guide listed a lot of browsers, which one should I use?

You can use any of the browsers we mentioned. For those who need a day-to-day browser, we recommend Firefox using the add-ons listed above. If you use Google Chrome or Microsoft Edge as a daily browser and don't want to switch, choose Brave. Brave is built upon the same core browser as Chrome and Edge and the same Chrome-based extensions can be used in Brave. We also list DuckDuckGo and Mullvad as options because these companies both have a relatively good reputation among privacy enthusiasts. We encourage you to try them all, or even use multiple if you feel it's appropriate. See which options you like and go from there.

Will this really help me prevent doxing or help me after I've been doxed?

It depends. This step when taken alone will not reduce your risk of being doxed. Tightening your security after being doxed or in preparation for a dox is not a bad idea. Switching to a fresh browser with limited extensions and clearing your browsing history regularly is one way to do this. For your current browser, you may be using an extension that may be collecting more data than it should or be malware; you may end up clicking on a phishing link and have your login or payment information autofill onto the page, or some data aggregator may have tied down your browser fingerprint to your identity, which may be available for purchase. It is possible, though not as probable, that someone may sell or publish this data which someone may then use to target you. It is more likely that someone targeting you will find your information from data brokers or based on what you've posted on social media.

The goal here is to limit your attack surface as much as possible so that should you ever be in a situation where you find yourself a target, your attackers won't have as much to work with. It is much more likely that most people will be doxed from information combed from their social media or through finding their information on a data broker website than from information leaked from their web browser. Despite this, through our experience

working with activists and human rights defenders, we frequently find people being attacked using novel and uncommon attack vectors. The effectiveness of these attacks can be reduced by taking simple steps to protect yourself.

Compartmentalization (for those with more severe security needs)

Let's say you typically use a single web browser. On this browser, you're signed into your social media accounts, your emails, and your online shopping accounts. Each of these services likely uses a variety of techniques to track your activity throughout the web. One of the primary (though not only) ways this is done is through cookies. Your activity can also be tracked via your browser's fingerprint, which is a set of characteristics about your device and browsing habits that may be unique to you or a small set of users. Switching all your activity to a different browser without changing your browsing habits will just create a new set of identifiers, or "fingerprint" still tied back to you.

If your goal is to make it more difficult for services to track you via your fingerprint, you may need to use a security strategy known as compartmentalization. This is a security technique in which you silo off different parts of your web activity so that they do not interact with each other. For example, using separate emails for your bank, online shopping, and personal life is a simple way many people already compartmentalize their lives. Applying this type of strategy to your web browsing activity may help to make it more difficult, though not impossible, to track you online. This strategy isn't guaranteed to work, requires a lot of effort, and may not be necessary for most people. You should create goals before compartmentalizing your browsing activity, as this is not a foolproof way to avoid tracking and there are still many ways you can be tracked. Examples of reasonable goals would be:

- Wanting to create a new social media account not tied to any of your other accounts.
- Not wanting to be tracked via cookies between different services you use and your activity online (though you may still be tracked via your fingerprint).
- Reducing your ability to be tracked via your fingerprint by using a separate browser and VPN connection to research a sensitive topic, or even researching something as innocuous as products to buy online while limiting advertisers' abilities to associate this information with you.

Many people already use "Incognito Mode" in their browsers. Nicholas De Leon from *Consumer Reports* has written a fantastic article about how Incognito Mode does and does not protect you from online tracking. We strongly recommend you go through this short and thorough article. Incognito mode makes it slightly harder for you to be tracked via cookies and your browser history because these are deleted when you close your Incognito window. Using Incognito may also *slightly* alter your browser fingerprint because typically it does not use any pre-installed extensions by default. This can be somewhat useful in compartmentalizing your browsing activity and should be adequate and easy to use for most people.

If your threat model requires you to take more severe precautions, another compartmentalization strategy is to use different web browsers in combination with different VPN-provided IP addresses for different *specific and limited* purposes. We want to emphasize that doing this can be complicated and may not prevent you from being tracked if done alone. This strategy is most appropriate for people experiencing a high level of threat, which specifically involves having information about their web activity purchased and used against them by a sophisticated actor. For most people, as of now, this is not a major threat, though that can change in the future especially if you've been doxed or otherwise targeted.

One way to implement this strategy is to utilize multiple web browsers, each with its own specific purpose. For this strategy to be the most effective, you need to fully close all other browsers from running and only use one at a time. This may look like doing the following:

- Assign Firefox to all activities regarding your finances, utilities, and shopping. Use the Firefox Multi-Account Containers extension to create containers for each of these activities.
- Close that browser completely when you are done with activities assigned to one browser. Then connect to a new VPN server, and open whichever other browser you choose for another activity, such as browsing social media.
    - If you do not wish to use a completely separate browser, assigning containers for other tasks may be sufficient. If you want more separation between these containers, be sure to close all other containers and switch your VPN server before opening a new one.
    - You can extend this practice for whichever silos you need to create for yourself.

This section may be confusing for some, as we discussed several different methods you can compartmentalize your browsing activity. Our goal in providing several options is to allow you to make the choice that is best for you. The three strategies we discussed are:

1. Use Incognito Mode, though only after understanding how it works
2. Use Firefox with the Firefox Multi-Account Containers tab and assign containers for specific tasks
3. Use entirely separate browsers with separate and specific purposes. Perhaps this can be used in conjunction with the above two methods
4. Always fully close your browser and switch your VPN connection before changing your compartment

While we discussed using compartmentalization to better protect your web activity, you can also apply this strategy to multiple aspects of your life.

Firefox Extensions:

uBlock Origin

Privacy Badger

HTTPS Everywhere

Firefox Multi-Account Containers

Facebook Container

Chrome Extensions (Also Works for Brave and Edge)

uBlock Origin

Privacy Badger

HTTPS Everywhere

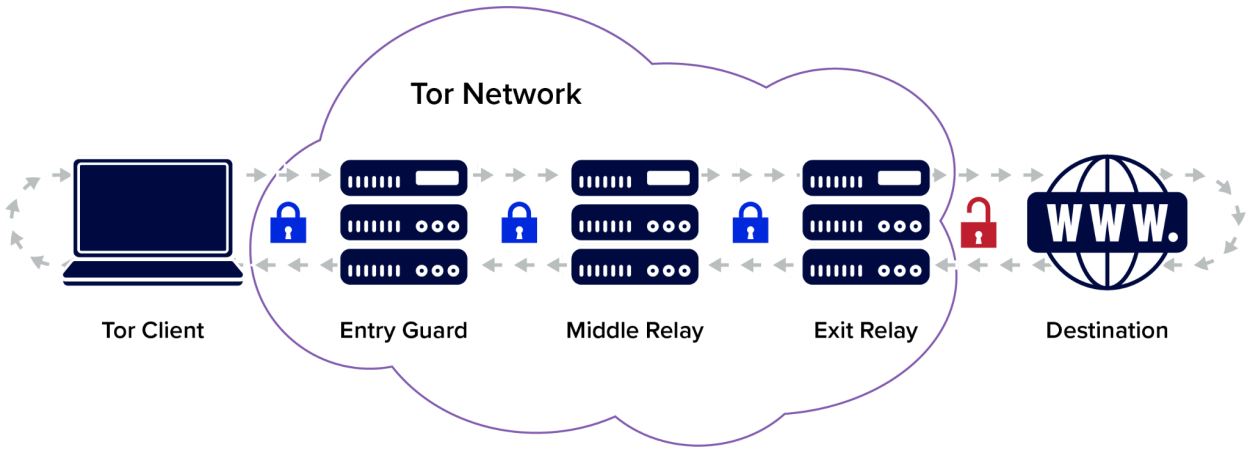
Additional Resources:

- Tool: Use a Recommended Web Browser - Consumer Reports Security Planner

- What Your Web Browser's Incognito Mode Really Does - Consumer Reports
- Data Brokers: Last Week Tonight with John Oliver (HBO)
- Device Info and Cover Your Tracks
- A prominent priest was outed for using Grindr. Experts say it's a warning sign.
- My Phone Was Spying on Me, so I Tracked Down the Surveillants
- Browser fingerprinting – tracking behind the curtain
- The Mullvad Browser hard facts: list of settings and modifications
- Leaked Documents Expose the Secretive Market for Your Web Browsing Data

Tor Browser Considerations

This section is for those who have a severe threat model though it contains information that may be useful to others. Using a VPN provides excellent protection for your online web traffic and general location, but rare and extreme circumstances may warrant a higher level of online protection. Those whose threat model involves being heavily surveilled by state governments or extremely sophisticated malicious actors may need to use the Tor browser for some online activity. Before deciding if Tor is right for you, be sure to read this section as well as the State Surveillance section of this guide.



Tor is a service that allows you to access the internet while also making it extremely difficult to trace a user's identity and other identifying characteristics, when used properly. This section is not intended to be a comprehensive guide to using Tor securely; rather, this discussion offers a starting point meant to assist those with elevated threat models who need to access the web safely. We strongly recommend contacting a security professional or conducting further research if you need to use Tor to engage in such activities as human rights work in jurisdictions where doing so may be criminalized.

When would you need to use Tor, and how should you use it?

You Should Use Tor If:

- You need to conduct business online without leaving any trace that would lead back to your identity.
- Your internet connection is monitored or censored by a corporation or government and you are a whistleblower or defender of human rights.
- You do not intend to sign into or create accounts with your real details such as your name, phone number, physical address, or email address.

You Should Not Use Tor If:

- You need to sign into a personal account such as your financial institutions, social media, or anything that can link back to your true identity when doing so would put you at risk.
- You intend to connect to a home network or non-public network affiliated with you or someone close to you when doing so would put you at risk.
- You are using a device that you believe is compromised by malware or that an adversary may have physical access to.

There are exceptions to many of these rules. Since this is a security guide for activists facing elevated threats, we are going to focus on a narrow use case.

How to Use Tor:

1. Know what you want to accomplish.

    a. Some examples of a goal could be using Tor to research your rights, post on an anonymous social media account not tied to your identity, or contact a trusted journalist using secure methods to blow the whistle on something.

2. Some jurisdictions criminalize the use of Tor or VPNs. To access Tor with a reduced risk to yourself, travel somewhere with public WiFi, far from your home, workplace, or school, and attempt to connect there. If the use of Tor is not criminalized in your jurisdiction, this may not be necessary.

    a. If you want to hide the fact that you are using Tor from your ISP, you may wish to use a reputable VPN before launching the Tor Browser.

3. Learn how to scrub metadata from documents, photos, and other files you may wish to upload through Tor. You can be identified if you skip this step.

4. Treat your activity on Tor as completely separate from your day-to-day life and identity. You should not sign in to any services that you usually access on your normal devices if doing so may put you at risk.

5. Close and reopen the browser each time you want to create a layer of separation between sessions

Risks of Using Tor:

The Tor network is frequently described as "anonymous" or safe, but there are still ways you can be identified by using Tor. If someone has physical access to your device, installed malware on your device, or if a sophisticated actor such as law enforcement conducts forensics on your device, it may be unsafe to use Tor. If you sign into an account tied to your personal identity or your personal devices, your activity on the Tor network may be traced back to you. If you use Tor while connected to your home network, your internet service provider will be able to know when you're using Tor and for how long, though they won't know what you are doing. If you use Tor while connected to a VPN, your VPN provider may know you are using Tor, though they won't know what you are doing.

For those wary of being heavily surveilled, using Tor could have devastating consequences in jurisdictions where access to the service may be restricted. Again, you should reach out to a trusted security professional if possible before engaging in sensitive work.

Tails OS (Operating System)

Tails OS is a portable operating system that routes all web traffic through the Tor network by default. Using Tails is ideal for anyone who believes their device may be compromised by malware or by someone with physical access. While it may seem a little complicated to install, Tails may suit your threat model.

Tails allows you to run the operating system from a separate media drive, such as a USB or disc drive, without leaving any trace that you've used Tails on that device. If you'd like to learn more about Tails and whether or not you may need it for your threat model, visit the additional resources in this section.

Additional Resources:

- Tor Browser for Windows - Online anonymity and censorship circumvention
- How Tails works
- Surveillance Self-Defense
- Warnings: Tails is safe but not magic!

Protect Your Phone

Encrypting your Mobile Device:

If your threat model includes the potential for a bad actor to gain physical access to your device, you should consider making sure your phone is encrypted and protected with a passphrase. Thankfully, most smartphones now come with encryption turned on by default. Encrypting your device makes it extremely difficult for an unauthorized third party to extract sensitive data from your phone when it is turned off. Note that if your device is currently not encrypted, there is a small chance that doing so may corrupt your data. Be sure to back up any crucial data you need.

Turning on encryption on your phone typically requires setting a passcode. When setting a passcode for your phone, you should once again consider your threat model. For best practices when setting a passcode, visit our Best Practices for Passwords section. You should also disable biometrics on your phone. For more guidance, review the section on passwords.

These measures are best for individuals who fear their device falling into the hands of law enforcement or another bad actor. Law enforcement can force you to unlock your phone via a fingerprint or FaceID, but they cannot legally force you to input your password. If you fear someone other than law enforcement may force you to unlock your phone, these measures may not be as effective. If you find yourself in this situation, we strongly encourage you to go through the Additional Resources underneath the Have You Been Doxed section.

Disabling Automatic Backups and Tracking:

One of the most common vectors of attack for someone under threat is the online backups (or cloud) created on a phone. For iOS users, backups are done via iCloud. For Android users, this could be done through Google Photos, Google Keep, and any of the other Google Suite apps. Backups are often created and maintained without the user's knowledge.

It is much easier for an attacker to go after your iCloud or Google accounts than gain access to the contents of your device itself. Law enforcement or other state actors can also easily obtain your data directly from Apple or Google with or without a warrant. Backing up via these services can be incredibly helpful in our daily lives, but the cloud can also be a massive liability if you are under increased threat from state or non-state actors. Consider disabling these features if you are experiencing heightened risk and have a good reason to believe your online backups can be compromised.

There are situations where maintaining good backups of your data, online or offline, may be best for your security. For example, if you believe your device may be physically confiscated by someone you live with or by another party, having a backup of your contacts, photos, and documents can be invaluable. iCloud also allows you to remotely lock any of your devices, while Android allows you to remotely lock or erase your device through your Google account, though doing so requires utilizing features that can affect your privacy (e.g., Find My and Location). While these features may have value to you, if you are under threat from law enforcement, enabling these features could put you at further risk. Ultimately you should determine which options work best based on your threat level and unique situation. For further consideration, check out Mozilla Foundation's *privacy not included to view the privacy and security of many apps.

iOS Settings

To Disable iCloud:

- Go to Settings
- Tap your name which should appear at the top of Settings
- Tap on iCloud
- Scroll down to "Device Backups" and ensure iCloud Backup is off
- Go back to the iCloud page
- Go to Show All
- Make sure everything that you want off is off. To disable iCloud completely, ensure everything is off

To Disallow Apps from Asking to Track Your Activity:

- Go to Settings
- Scroll down to Privacy & Security
- Select Tracking
- Turn "Allow Apps to Request to Track" off

Android Settings

To Disable Automatic Backups:

- Go to Settings
- Go to Google Services & preferences
- Go to Backup
- Do not allow backups

To Disable Photos From Being Uploaded Online:

- Open your Photos app
- Click your Gmail Profile Picture (the upper right-hand of the screen)
- Turn off Backup

Disable Google Activity Controls:

- We provide instructions on how to do this on a web browser here
- On your Android device, go to Settings
- Go to Google
- Select "Manage your Google Account"
- Follow the steps we discuss here to help you conduct an audit of Google's privacy settings

To Disable Personalize Using Shared Data:

- Go to Settings
- Go to Google
- Go to "Personalize using shared data"
- Turn everything off

To Disable Google Contacts Sync:

You may find this setting useful to back up your contacts. If you are not comfortable using this feature and want to back up your contacts manually, there are several ways of doing so.

- Go to Settings
- Go to Google
- Go to "Google Contacts sync"
- Ensure your contacts are not being synced

Protect the Data on Your External microSD Card:

- If you use an external microSD card to expand the amount of storage on your phone, it may not be encrypted even though your internal storage is
- Make sure you backup any files you are about to encrypt as this process will likely erase all the files on your microSD card
- Your Android device likely has two options for formatting your external microSD card: For portable use or for internal use
- Be aware that, while it may be useful in some cases, formatting your external microSD card for portable use will easily allow anyone to see the data written onto it.
- If you want to make it harder for your data to be extracted, format your microSD card for Internal use instead.

Use End-to-End Encrypted Messaging Apps

Consider using the app Signal for your sensitive communications. This secure messaging and voice app can take the place of text, phone, and e-mail when installed on your phone. You must first install it on your phone (for iPhone and Android devices) and make sure you verify your account with your phone number. Alternatively, consider using Wire as a secure messaging service. Wire only needs to use an email as a verification method, so your account is not tied to your phone number. Apps such as WhatsApp and Wickr, despite being end-to-end encrypted methods of communication, may still retain and

distribute data on their users. Regardless which secure messaging service you adopt, we also recommend that disappearing messages be turned on for any potentially sensitive conversations. This feature means that messages will be automatically deleted after the amount of time that you set. When choosing that interval, be realistic: Don't set it too short (or you run the risk of not everyone seeing the message), but be careful not to set it too long (as that can defeat the purpose of the disappearing messages).

Additional Reading:

- What is Secure? An Analysis of Popular Messaging Apps

Protect Your Phone Number

After you've been doxed, it's extremely common for your phone number to become the primary point of attack for your harassers. You might receive disturbing messages, phone calls, and images against your will. Attackers can also try and engage you in a phishing scheme or try to take control of your phone number through a SIM swapping attack. This can allow an attacker to pose as you by using your phone number and likely gain access to your important accounts.

Porting Your Phone Number

Consider porting your phone number to a VOIP (Voice Over IP) service, which essentially moves your phone number from a standard cellular provider, vulnerable to attacks, to an online-only provider that is much more difficult to compromise. Porting your number will allow you to control when and how you receive calls and messages, better log incidents of harassment or threats, and prevent an attacker from gaining control of your phone number. We strongly recommend Google Voice as the simplest way to port your phone number. If you don't like this option, don't worry; you can always port your number to another service later, including back to your cellular provider if you wish.

There are a few things to consider before porting your number. This process typically involves contacting your cellular provider and paying a fee to the provider you wish to switch to. It also means that once your phone number is ported, your mobile device will likely no longer have service, and you likely need a new plan or phone number from your old provider to continue using your device as intended. It is best to conduct this process while your phone has a WiFi connection. Finally, after having been doxed, you should be extremely careful about sharing any new phone numbers you obtain.

Obtaining a Secondary VOIP (Voice Over IP) Number

Using a second phone number through VOIP, aka a digital phone number, offers an extra layer of protection from certain threats. If you are concerned that unencrypted messages may be released or obtained through your cellular service provider, using a VOIP number such as Google Voice, MySudo, or Burner App will allow you to communicate without leaving records through your provider. Remember that someone may still be able to view these messages if they gain access to your device.

You can also use a burner number to sign up for things that you don't want linked to your real information. Using VOIP services still carries some risks, especially when tied to your mobile device or true phone number, which almost all VOIP providers require. These companies are legally bound to respond to subpoenas from law enforcement, so they could potentially release incriminating data that ties directly back to you. Below are some simple VOIP options to help get you started:

Google Voice (Google Voice)

- Great if law enforcement isn't a concern; do not use it if it is.
- Extremely difficult to set up without connecting your true cellular number to your identity. Best to set this up before porting your original phone number for verification purposes. After switching your account to use an app-based 2FA option, you can delete the phone number from your Google account.
- Highly likely that user data is sold.

BurnerApp (Burner)

- Again great if law enforcement isn't a concern or set up in such a way it cannot be tied back to you.
- Definitely sells user data.

MySudo (limited free numbers) MySudo

- Again great if law enforcement isn't a concern.
- Does not require the use of your cellular number, though still requires a smartphone.

- Users can delete messages and calls from MySudo.
- Can be pricey beyond their limited free option
- Fairly easy to set up

Twilio (Twilio)

- Cheapest option but also less accessible
- Difficult to create an account sometimes

Do You Need a Burner Phone?

In extreme and limited circumstances you might consider utilizing a second phone for specific purposes, often referred to as a burner phone. We believe the overwhelming majority of people do not need to go through the costly and cumbersome steps to obtain one. If you've been doxed, porting your phone number and obtaining a new one should sufficiently protect you from most attacks. The decision to obtain a burner phone is a very personal one that ultimately only you can make after carefully conducting a personal threat assessment. If you feel you need a burner phone to address your specific security needs, continue to read the rest of this section. If you feel that you do not need a burner phone, feel free to skip this section.

Doxing can lead to increased attention from highly sophisticated threat actors. In rare though not uncommon circumstances, these threat actors tend to be nation-states. It may also be possible that a less sophisticated actor has physically accessed your phone and installed malware on it without your knowledge. (This is most commonly seen in abusive relationships.) These are some instances in which a properly configured and obtained burner phone can mitigate some risk depending on how it's used.

Setting up a proper burner phone is extremely difficult even for professionals. Before considering if you need a burner phone, ask if it fits within your threat model. Here are some questions to consider before deciding whether a burner phone is right for you:

- Do you live in a jurisdiction where exercising certain rights is heavily surveilled or criminalized, and do you absolutely need to bring a phone to events such as a protest where you suspect mobile device surveillance will be conducted?
- Do you have reason to believe that you are under surveillance by a highly sophisticated actor, such as a nation-state? While this can be rare, journalists,

human rights defenders, politicians, lawyers, and activists advocating for certain causes are at higher risk for nation-state surveillance

- Have threat actors discovered your new phone number that you did not advertise anywhere after porting your old phone number to a VOIP service?
- Do you believe your phone has been targeted by stalkerware by a partner or someone else in your life? (if so, please read the resources in this or this section)
- Are you able to keep your burner phone off, hidden, and completely separate from your day-to-day mobile device?*

If you answered yes to any of these questions, you may benefit from using a separate burner phone. Keep in mind, doing so takes a lot of planning, time, and resources.

Before you purchase a phone, keep in mind that this phone is to be completely separate from your personal life. **A burner phone should never be around your personal phone, nor turned on within a certain distance of your home.*** A burner phone can also be difficult to hide from a partner or someone else you live with. If you are being surveilled by a nation-state actor, using a burner phone may not prevent all surveillance against you as your phone is likely not the only thing of yours being surveilled. If you are using SMS to send text messages on a burner phone and are being surveilled by a state actor, your communications may still not be safe.

Setting Up a Burner Phone

When going to purchase a phone, leave your own phone at home and visit a store that sells unlocked phones (e.g., Target or Best Buy). You may also have some luck purchasing a prepaid phone, which comes with an activation kit that can be activated via public WiFi.*

Consider your options: Do you need to use apps, such as a navigation tool or end-to-end encrypted communication? Or do you just need a phone number? The answer should determine whether you should get a cheap smartphone or a simple flip phone.*

Note: DO NOT log into any accounts associated with your true identity on this phone. There are very few exceptions to this rule, and the risks of doing so are highly dependent on your situation.

If you envision using safe end-to-end encrypted messaging, such as Signal, or require the use of a navigation app, you may need a smartphone.*

Pay only in cash.*

Research cellular services that do not require signups. Avoid service providers that require a credit check. See if you can find prepaid SIM cards that can be activated online. (You can use the phone you just purchased and public WiFi from a coffee shop or library to do this.)*

If you live near a Best Buy or a Target, your easiest option will likely be a Mint Mobile 7-day free trial SIM kit. The phone can be activated online and provides a very limited talk, text, and data plan for seven days. If you need a little more data, you can purchase a three-month prepaid SIM. Your mileage with other prepaid SIMs may vary.*

If you bought a smartphone, use public WiFi to configure it. You can use your new phone number to sign up for iCloud or Google if you need to use other apps. Remember to use an alias when creating these accounts, and remember that this phone should be turned completely off as soon as you're within several miles of your home for most people. Do not use an iCloud or Google account already associated with you.*

Do not use this phone to download social media apps or other apps you do not absolutely need. Never sign into any of your normal accounts using this phone. It should only be associated with an alias.*

Do not use this phone to contact people unless you exclusively use secure messaging apps such as Signal, Session, or Wire. Know the risks of what could happen if another party obtains this phone. Your messages may be end-to-end encrypted, but that does not stop someone from physically taking your phone and reading your messages. If you are at risk for this, be sure to enable disappearing messages on all your communications.*

Do not use this phone to contact people outside of secure messaging apps which require data. Doing so can create a trail leading back to you.*

If you are attending a protest and cannot afford to turn the phone off or must turn it on at certain points, be sure to do it while you are not at risk of having the device confiscated. It's also a good idea to keep Bluetooth, WiFi, and your location turned off. **Keep in mind that if this device is confiscated, it could not only expose you but also others.***

Keep in mind that even after using all of these steps, configuring a burner phone leaves a lot of room for error, which is why we recommend you explore other options.*

Properly dispose of the phone when you are finished. It's generally recommended you do not keep or sell the phone. It's called a "burner" for a reason.*

* There are some exceptions to keeping your burner phone and personal device completely separate. A good example of where this is not necessary is in abusive relationships in which someone, usually a partner, has control over your personal device. Keep in mind that in these types of situations, a burner phone might increase the risk of violence if it is discovered by an abusive partner. If you are in an abusive situation, it may be safer to keep your burner phone with a friend, at your workplace, or opt for not using one if you are not sure you can keep it hidden. If any of this resonates with you, please visit the links in the additional resources section on a secure device, preferably either a work device or the device of a trusted friend.

Compromising a Burner Phone

Even when someone follows the strictest security protocols in obtaining a burner phone, there are still many ways anyone can be compromised while using a burner device. If you are being physically surveilled by a state actor it won't take long for them to discover the existence of your burner device. If you make a mistake, which is easy for even professionals to do, you may end up creating a compromising trail from your burner identity to your true identity. If you use such a phone during a protest, law enforcement may still be able to use that phone's general location along with other surveillance means to identify you or others associated with you. If this phone is confiscated, especially if it is not encrypted and turned off, the confiscator will easily gain access to all your communications and activity even if you use E2E messaging apps such as Signal.

There is a lot of room for error here. We want to re-emphasize that very few people may need a device such as a burner phone, and those that need one should consult with a security professional if able.

Additional Resources:

- What to do if your phone is seized by the police
- My partner is monitoring my computer or cell phone activity.
- Tool: Remove Stalkerware - Consumer Reports Security Planner
- Resources-Survivors — Safety Net Project
- Warning signs of abuse
- Coalition Against Stalkerware (EN)
- Research Archives - The Citizen Lab

Use Encrypted Email Providers

Chances are you've been using a mainstream email provider such as Gmail, Outlook, or Yahoo. While many of these providers offer robust service, they all have one major flaw: the lack of end-to-end encryption (E2E), at least as of this writing. If you're not sure what this means, this Business Insider article offers a quick explanation: Basically, the contents of your email accounts may be seen by unwanted third parties.

These companies also comply with requests from law enforcement to turn over any or all the information they have on you, which is especially a concern for human rights activists who may be targeted by state actors. Gmail in particular has also been known to collaborate with government surveillance programs, such as the NSA's PRISM project. This is especially a concern for individuals whose threat model involves protecting themselves from state actors or anyone who cares about privacy.

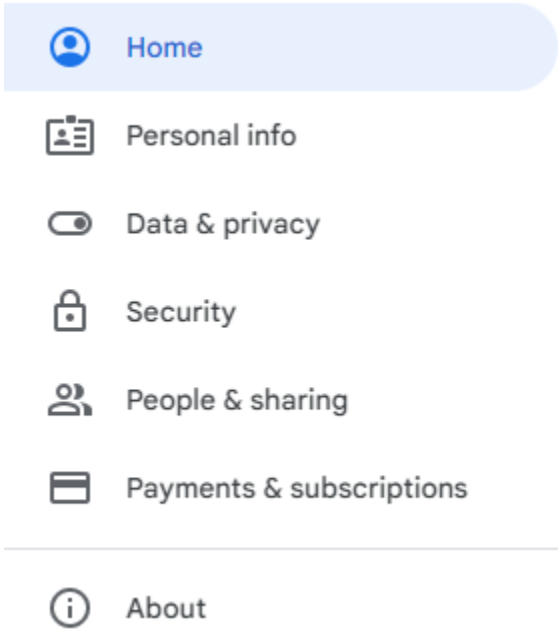
The best way to secure your email is by using a provider that offers end-to-end encrypted services, such as ProtonMail or Tutanota. Both companies are zero-knowledge providers, which means they are unable to view the contents of your messages. Only someone with your password (and hopefully 2FA key) can view the contents of your account.

Switching to secure email can be helpful for individuals who have been doxed and/or are experiencing harassment campaigns. While E2E email providers must also comply with law enforcement, the information they can turn over is extremely limited. If this risk is included in your threat model, take precautions, such as using Tor or a reputable VPN to log into these services. Ultimately, only someone with your login credentials can view the contents of your messages. If you've been following our guide, your process should look something like this:

1. Choose a password manager.
2. Immediately change the passwords for your most crucial accounts; start with your primary emails, socials, and financial institutions; check HaveIBeenPwned to help you prioritize the rest of your accounts.
3. Choose a two-factor authentication method, preferably an app such as Authy or Google Authenticator, and turn on 2FA, following the same priority of accounts.
4. Create a Proton Mail or Tutanota account.
5. Have all your old emails redirect incoming messages to these accounts if you like.

Check your Google Account Settings

While they provide great services, Google has been criticized for collecting immense amounts of data on its users and storing information without users' explicit knowledge. Your Google Account may have information about your location, what apps you use and when, and your search history since you created your Google account. This information can be used against you if a bad actor compromises your Google account. Even if you've already changed your Google password and are using 2FA you should also take these steps: Visit https://myaccount.google.com/. In the upper left-hand section, you should see these options:



These settings can contain information you may wish to have deleted or no longer collected. Be sure to go through each one to determine what you want to have visible to whom, what data you allow to be collected, and what data already has been collected that you want to remove.

The most worrisome settings are under "Data & Privacy." Here you can see whether or not Google has been collecting your location history, delete whatever they have collected, and instruct Google to no longer collect this data. You should do this for all your Google accounts, especially if you have ever used an Android phone or frequently use Google Maps.

If You Cannot Use an E2E Email Provider

There are situations where someone can't use an end-to-end encrypted email provider. More often than not this applies to people who live in jurisdictions that criminalize free access to such services. If you cannot access an encrypted email provider, you may want to consider manually encrypting your communications over email via GPG Encryption. Setting up your own form of encryption will generate a set of keys that will allow anyone with access to encryption software, such as GNuPG, to encrypt their messages to you and vice versa. Setting up this software can be intimidating, but there are many resources out there to guide you. Please note that in some jurisdictions, use of this software may also be criminalized.

Popular E2E Email Providers:

https://Protonmail.com/ | Secure and Encrypted Email

https://tutanota.com/ | Secure Email

Additional Resources:

- Privacy concerns regarding Google - Wikipedia
- Google's Privacy Backpedal Shows Why It's So Hard Not to Be Evil - The New York Times
- Email Self-Defense

Utilize More Secure Options For Group Communications

After being doxed, it's not uncommon for trolls to uncover what communication platforms you use and attack them. This can include Discord, Skype, group DMs on social media, and many others. If you've been following along in this guide so far, you should have already changed your passwords and turned on 2FA for these services. Doing so will make it much more difficult for an attacker to compromise these platforms.

Even if you follow all these steps, an attacker could still compromise the security of your Discord server or gain access to a Zoom call you or your work may be hosting. You may want to consider hardening the security and privacy settings of these services or switching to an alternative group messaging/conferencing platform altogether. It's especially important to pay attention to any new members on a Discord server or unrecognized names on a Zoom call.

For group messaging we strongly prefer Signal. Signal has a robust group chat option that allows you to turn on disappearing messages, verify who is in the chat via their phone number and Signal Safety Number, and also allows for group calls. If you need the capabilities that typically come with conference calling software, consider using Jitsi. Jitsi is a free alternative to products like Zoom. Creating a room does not require the creation of an account. You can send an invite to anyone you trust and also set a room password. Jitsi also has a feature that allows you to encrypt a call if needed.

Both Signal and Jitsi are great options for those whose threat model includes the possibility of infiltration by a bad actor and for those whose data may be subpoenaed by law enforcement. There are still plenty of ways the security of these two platforms can be compromised depending on how you use them, but in general, these options should suffice especially during times of elevated threat.

Change Your Privacy Settings on Your Social Networks

Visit your privacy settings for Facebook, Twitter, Snapchat, and Instagram to make your accounts private and block all trolls who already follow you. In some cases, you may wish to block any account you are unfamiliar with or accounts belonging to individuals you have never personally met.

For LinkedIn, note that professional connections can be at particular risk if they are found to be engaging in political activities. To disable the public visibility of your profile, go here and on the right-hand side you will see “Your profile’s public visibility.” Switch this setting to “off.” Further information can be found here.

Facebook privacy settings can be found here.

1. Change your settings so that only your friends can see your current posts. When you want to post something work-related as public, set those individual posts as public. Protect past timeline posts by watching this video.

2. If you can, review your friends lists. Unfriend all those people you can’t remember or maybe vaguely remember some awkward interaction with them. Double-check that each of your friends is unique and no one has created accounts with similar names and photos of a real friend.

3. Go through your profile information and make sure your phone number and email are set to be viewed by “only you.” Remove featured photos and/or any information in your “About” section in your profile that you would not want to see appear on doxing sites. Often trolls will take your album photos and spread them across the internet. They will do this to either create a fake profile for you, or make harassing memes or messages about you.

4. Remove your Facebook public photo and replace it with a generic photo that doesn’t have your actual picture. Also, remove your full birthday or replace it with inaccurate information.

For Twitter, take the following actions:

1. In your account settings, make sure you have 2FA, and verify all login requests so you can flag anyone trying to access your account.
2. In your Privacy and Safety Settings, make sure you turn off your location settings. This prevents you from leaking your location through your Twitter status.
3. Turn off Photo Tagging, so that random troll accounts can't tag you in harassing content or comments.
4. Turn off discoverability by email or phone.
5. Finally, if you feel it's necessary, make your account Private.

Other social media platforms can make it difficult or confusing to change your privacy settings. If the above instructions no longer work or you're having trouble finding the appropriate security and privacy settings for your platform, we encourage you to take some time sifting through all the available settings offered to you. This can be difficult and frustrating, but the results are worth it.

Delete Your Data

Deleting an account does not delete your data, and you must request the removal of data **before** you delete your account. In general, you can find information on data removal in the privacy policy of an app or service's website. You can search the Privacy Policy for words like "removal," "delete," or "opt-out" by holding the control/command keys and F key together.

Sometimes navigating privacy policies for companies can be tricky. Many companies that sell your data have a vested interest in making it confusing or difficult to remove your data. If you do not see clear instructions on how to delete your data from a company's privacy policy page, you can typically find an email for inquiries.

If you're from California, live in California, or have ever been to California, you may be able to have your data removed through the CCPA. The CCPA is a California State law that requires companies to comply with their users' request to see their personal data, stop the sale of their data, or delete their data if they request it. Search for "CCPA" or "California" on the security policy page and follow the instructions to have your data removed. You can send a message to that email with the subject "CCPA Request for Deletion." Here's a sample request::

> "This is a CCPA request for the deletion of all data associated with this account [insert account here]"

Legally, the company must comply with a request to delete your data, yet many companies have shady privacy practices and may continue to retain or collect new data on you from other sources. The safest thing to do after sending a request for deletion is to discontinue using the account. If you're not sure this will work because you are not from California, it may be worth it to try as many companies will honor CCPA requests without verification of residence.

Kill All Unused Accounts

Remember trolls are going to use whatever information they have to access your accounts. Accounts you have not used in a long time can leave you vulnerable, especially if they have an older password. Be on the safe side and shut them down. Deleting your unused accounts may be simple, but finding and remembering them is often challenging. Here are a few methods to locate accounts:

- Search your email threads.
- Use search terms that might appear in an account sign-up or verification.
- Search specific platforms.

- Search your web browser and review the “Passwords” or saved logins on browsers like Safari, Chrome, and Firefox.
- Review data breaches by consulting websites like haveibeenpwned.
- Check bank statements for recurring accounts you might have forgotten.
- Within your social media accounts, check if you have granted any third-party access to link with other accounts.

If you can’t delete the account, you can at least try to make it useless to an adversary. Remove any sensitive information like your name, address, and payment info. Deleting accounts does not delete the data, so check for data deletion policies and procedures. Delete your private data within the service, and if possible, change the account information to an alias. You can get a list of accounts that you may have forgotten by using the tool, Namechk.

Further Reading and Resources:

- JustGetMyData
- AccountKiller

Use Aliases When Signing Petitions or Sign-in Sheets for Meetings

One of the most common ways people find their names on doxing lists is through petition websites and sign-in sheets. We recommend that you **never** use real names, phone numbers, or e-mails for these kinds of activities. A common way to continue participating in public processes such as petitions or email campaigns is to create a nickname for yourself. This is a name you can use to identify yourself without giving away the name you were assigned at birth. You can choose any nickname you wish, though be sure to compartmentalize this name from your true name.

Once you've chosen a nickname you should create an email account associated with only this name and not your name assigned to you at birth. Use this name when you need to fill in a sign-in sheet or sign a petition. You can also create a phone number for this identity if you need to. Consider using Google Voice or a burner app like MySudo to avoid divulging personal information.

Protect Your Computer

Aside from our mobile phones, most of our digital activity tends to take place on our computers. Many people who have recently been doxed tend to see a sharp increase in attacks that attempt to gain access to the information on their devices. In this section, we walk you through best practices to secure your device against a wide array of attacks.

Keep Your Computer in Your Possession

Many people overlook the fact that having physical possession of your devices at all times is a good security practice to normalize. Leaving your devices unlocked and unattended at a coffee shop, in a meeting, or at school while you leave the room can leave them vulnerable to theft or malicious tampering. As a best practice, do not leave your devices unattended in public areas. We encourage you to not only shut and lock your devices but also take them with you when leaving a room. While this can seem overly cautious, maintaining physical control of your devices is the only way to ensure they aren't physically compromised or stolen.

Keep Your Computer and Software Up to Date

Whether you use Windows, MacOS, ChromeOS, or any distribution of Linux, the best thing you can do to secure your device is ensure you regularly check for updates on your computer and any software you may use. This can include web browsers, word processors, email clients such as Outlook, and whatever other software you use on your devices. Additionally, we tend to recommend some plugins to your browser like PrivacyBadger, HTTPSEverywhere, and uBlockOrigins

Install and Regularly Update Antivirus and Malware Protection

Many devices come with malware protection built in. Windows comes with Windows Defender, while ChromeOS and MacOS have other native tools which are capable of detecting and dealing with malware as long as you keep the operating systems updated. If you're on Windows, Windows Defender is adequate for most users. We tend to recommend utilizing VirusTotal in addition to Bitdefender or Malwarebytes for Malware and Antivirus.

Turn on Your Firewall

A firewall helps to ensure that no unauthorized web traffic enters or exits your device. We strongly recommend checking the firewall settings of your device and ensuring that it is turned on.

Consider Partitioning

Consider creating separate user accounts on your desktop or laptop. If configured correctly, this may allow each user extra privacy on your device. Please reach out to us if you need further technical support or have questions about how to do this.

Use a Strong Passphrase or Password

Use the advice from our Password section and apply it here to create a strong, unique password or passphrase for your device.

Use Encryption if Possible

While your device may require a password to log on, an adversary or someone who steals your device may easily be able to access the contents of your computer if you do not utilize encryption as part of your security strategy. We recommend you use Full Disk Encryption (FDE) when possible to secure the files on your device. This way if your device gets stolen, the data on it will likely be inaccessible to anyone without your password. This is especially important if you have important documents on your device.

If you are running a Professional version of Windows, you should have access to BitLocker, which is Windows's native way to encrypt files on your system. If you're running MacOS, you should have access to FileVault. ChromeOS is typically FDE by default. Keep in mind that if your device is not fully encrypted, encrypting it can take a long time and there is a small chance that some of your files may be corrupted and this may result in you needing to reformat your system. Before deciding to encrypt your system, be sure to back up any important files.

If you do not have a Professional version of Windows, you may need to look at other options for encrypting your data. Third-party software, such as Veracrypt, can allow you to fully encrypt your device or encrypt specific files of your choosing without using BitLocker. Using this software can be a little complicated for those unfamiliar with it, and using it may run the risk of corrupting some or all of your data. Before encrypting anything, be sure to back up all your important files.

While utilizing encryption can be a great security strategy, you should do your best to conduct your own research before deciding if this option is right for you.

Review Your Privacy and Security Settings

On Windows

- Go to Settings
    - Go to Privacy
    - Turn everything off
        - On the sidebar under "Windows permissions" go to "Activity History"
            - Make sure every box here is unchecked

- On the Sidebar go to "Diagnostic & feedback"
    - Select "Required diagnostic data"
    - Turn off Tailored experiences

Cover Your Webcam When Not in Use

If your device does become compromised, an attacker can look through your webcam without you ever knowing. Most computers now come with a built-in physical slider that covers your webcam. If you do not have one of these, many cheap and effective webcam covers are available for purchase. If you have an external webcam, it likely already comes with a slider to cover the camera when not in use.

Antivirus and Antimalware

Malicious software (malware) is most often installed on a device by tricking you into clicking a link. Using antivirus software and keeping your devices' operating systems updated will help to protect against some methods of malware installation, but some targeted implementations of malware (e.g., government level) may be more sophisticated than what standard antivirus software can detect. Always carefully inspect anything you might consider clicking as a first line of defense. **Do not** click on any suspicious links, attachments, or pop-up windows. Use a service like VirusTotal to check the safety of links and files before opening.

Malware can also spread through unsecure networks like public WiFi. Using a VPN on public WiFi helps protect information on your device. Avoiding signing up for free services like VPNs or file-sharing, which may gain access to the contents of your device while connected or in use.

Indicators of a compromised phone or computer could be unknown IP address access, audio/video recording indicator, and performance issues. You may find that your browser searches redirect to a different page; there are new apps downloaded; or operating system tools are disabled or blocked. Highly sophisticated malware can go undetected with no indications of its presence.

Advanced technology users, however, may conduct their own digital forensics to detect and/or remove malware: GitHub - mvt-project/mvt: MVT (Mobile Verification Toolkit) helps with conducting forensics of mobile devices to find signs of a potential compromise.

Protect and Backup Your Hardware

The final step is to get an encrypted external hard drive and/or secure cloud services to back up all your personal data and software. This greatly reduces the chances of losing access to valuable data. If you need to protect your backups from being accessed by anyone other than yourself, you may wish to encrypt it using the steps listed here. Both Windows BitLocker and VeraCrypt can be used to encrypt all or portions of external drives.

Some examples of external backup options are:

- SanDisk Extreme Portable SSD
- Western Digital 5TB Passport Hard Drive
- Sync - Secure Cloud Storage
- Box - Secure Cloud Storage

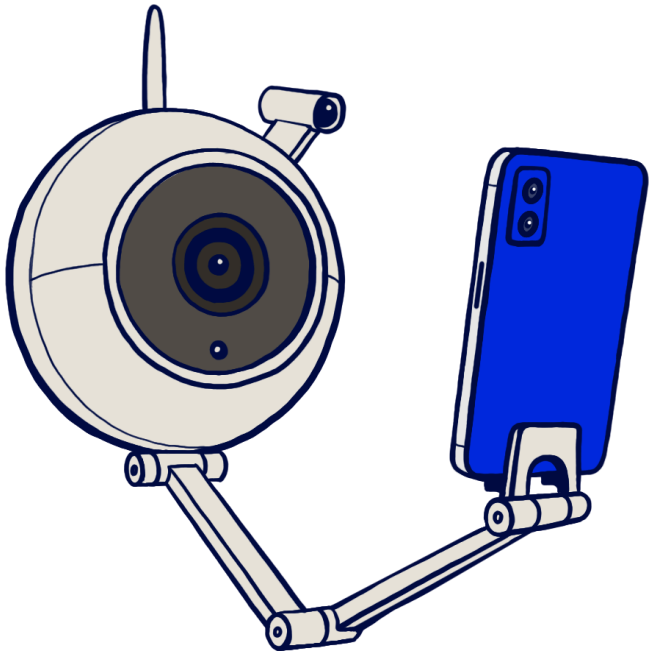
If you have any questions, contact us on Instagram, Twitter, or Facebook.

State Surveillance and State Doxing

State surveillance can be performed overtly or covertly with different goals. Overt surveillance intends to have a “chilling effect” on activists to self-censor their words and actions out of fear. One example is home visits which serve mostly to let activists know they are being monitored. Covert surveillance is more of what we deal with in this guide.

Typically, covert surveillance is conducted to gather and analyze information about an individual or group. Covert surveillance includes methods like issuing subpoenas for data, or utilization of technologies like wiretapping and internet scrapers. Use of

deception, social engineering, informants, or agent provocateurs can also be used for covert surveillance, so be sure to only share sensitive information with people you trust and through methods that cannot be intercepted or easily accessed, such as end-to-end encrypted messaging or other secure means.



While state agencies like the FBI or NSA have the most resources available for surveillance, local law enforcement agencies have increasingly gained access to more militarized tools and equipment. To check some of the surveillance technology being used by your local police department, check the EFF's Atlas of Surveillance, which "includes drones, body-worn cameras, automated license plate readers, facial recognition, and more."

State surveillance is different because LEOs have access to more sophisticated methods and publicly unavailable information. While some tactics are straightforward, like purchasing data from data brokers, others include the use of technology that can collect, store, and analyze information about targets, such as CCTV and facial recognition databases, such as ClearView. Some of the advice in this guide can already help disrupt common forms of state surveillance and information gathering.

Another way state surveillance differs from a non-state bad actor is the resources and capabilities at the disposal of the state, including mass surveillance of a protest that spans several blocks. Methods of mass surveillance can include the interception and collection of data during transit (unencrypted communication), mining and analyzing data

scraped from the public internet or private databases, and equipment like imaging technologies or cell site simulators which replace cell towers with their own closer (and monitored) signal and can reveal information unique to each cellular device.

Consider your threat model as **the majority of activists are not being actively monitored by the state**. Think about the most likely strategies that may be used to surveil you and what information of yours is most vulnerable or easily obtained. While mass surveillance can be conducted across the population for any reason, targeted surveillance often suggests some amount of prior suspicion. Targeted surveillance may include phishing, issuing subpoenas/warrants for data, physical surveillance of your home, or targeting your devices specifically. We have little to no control over the state's abilities, but we can make it harder for others to access our data and information.

Some regions have already banned the use of facial recognition technology. Strong digital security practices can help defend against government catch-all data collection, with extreme cases involving the physical or remote installation of malware/spyware. That being said, when extremist actors engage in targeted harassment of activists, state actors will often begin monitoring the activist(s) that have already been doxed. Don't be discouraged, do what you can, and support each other.

Takeaways: Look for digital security options that have demonstrated a strong resistance/process regarding: warrants, protect your search/browser history, use VPN on mobile data, use encrypted communications, scrub data, leave your personal device at home during protests.

SIM PIN? Feds Are Tapping Protesters' Phones. Here's How To Stop Them

How to defend against mass state surveillance like palantir/Clearview? Is there any way out of ClearView's facial recognition database?

- Keep info off the public internet that is scraped, use smart profile/cover pics that are always public, limit account visibility as much as possible.
- Keep others safe—do not post identifiable photos of people without their consent, encouraging this practice also benefits you when others ask to share a photo you're in.
- Review privacy settings of social media/online platforms about their data policies.
- California residents can request to view/delete their info from ClearView under the CCPA, but remember that data can be accumulated again.

What Does State Doxing Look Like?

One example is the release of mugshot photos of protest arrestees with other identifiable information like name, age, and region of residence. While the stated intent of police departments to broadcast this information may be for “public safety,” this tactic is used inconsistently. When done during times of political unrest, this dangerous practice has led to further activist harassment (and harm/doxing?) by non-state, far-right bad actors. If you have reason to believe you could be arrested at an action, regardless of your activity, and would be concerned about your information being released, you can preemptively secure your info/privacy by not having your personal device with you, and making social media accounts private or deactivated. Covering your face or tattoos will also help reduce the data gathered about you if there are cameras around.

Further Reading and Resources:

- Defend Dissent by Glencora Borradaile
- Trolling, doxxing and false arrests: How governments are using tech to intimidate critics in Southeast Asia
- D.C. Police Closely Watched Anti-Racist Groups for Years
- Tunisian police are using drones and Facebook to doxx LGBTQ protesters
- FBI Hired Social Media Surveillance Firm That Labeled Black Lives Matter Organizers “Threat Actors”
- How Domestic Spying Tools Undermine Racial Justice Protests | Freedom House
- Surveillance Self-Defense

Additional General Anti-Doxing Resources

1. CrimethInc: Prevention and Aftercare for Those Targeted by Doxxing and Political Harassment

2. Electronic Frontier Foundation Surveillance Self-Defense
3. Electronic Frontier Foundation: Tips To Protect Yourself Online & How to Minimize Harm
4. Electronic Frontier Foundation: Cover Your Tracks
5. Digital Defense Fund: Learn — Digital Defense Fund
6. Tactical Tech: Safety First! — The Kit 1.0 documentation
7. TechPolicy: What is Secure? An Analysis of Popular Messaging Apps
8. Palante Tech: Zoombombing Digital Community Security in the Age of Coronavirus
9. Palante Tech: Zoombombing Self Defense: Technical Guide
10. ACRE Public Share: Resources Against Zoombombing
11. TechSoup: Keeping Your Nonprofit's System Secure During COVID-19
12. Frontline Defenders: Digital Security Resources
13. Crash Override Network: Crash Override Resources (outdated)
14. Hacking//Hustling: Hacking//Hustling
15. New York Times: A Guide to Doxxing Yourself on the Internet
16. New York Times: Doxxing Curriculum Guide
17. New York Times: Social Media Security & Privacy Checklists
18. Library Freedom Project: Preventative Measure Checklist
19. PEN America: Online Harassment Field Manual
20. Google: Remove select personally identifiable info or doxxing content from Google Search
21. IGD: We Are Being Doxxed
22. IGD: Guide to Using Signal Securely

23. Regent University School of Law: Don't Talk to the Police
24. Gimlet Media: How to Avoid Being Tracked by Facebook
25. Terms of Service; Didn't Read: ToSDR
26. Consumer Report: Security Planner
27. ZNET: How to delete yourself from internet search results and hide your identity online

We know that this is a lot! Keep in mind digital security is a system that you are creating and implementing as part of your core skills as an organizer. There is no silver bullet to digital security: it is an awareness and a practice that gets better with reiteration and with a community committed to staying safe. **The best defense is a collective one, and we are all in it together.**

If you have any questions, comments, or concerns **please feel free to contact us:** inquiries@equalitylabs.org