Doxcare

Prevention and Aftercare for Those Targeted by Doxxing and Political Harassment

CrimethInc.

August 26, 2020

Contents

This step-by-step guide explains how to protect yourself from online stalkers, why it is important, and what to do if you are targeted for "doxxing"—the publishing of your private information. In a era of universal surveillance, when livestreamers broadcast every major demonstration while fascists, FBI agents, and police officers comb through social media posts to gather intelligence with which to harass activists, there has never been a better time to take steps to secure your privacy. Here's how.

Introduction: One Person's Story

I have been active in my community for years. Not long ago, far-right trolls found social media accounts of my friends, family, and workplace. They stalked me and used the photos they found of me and my family members to assemble timelines of my life and to map my social networks. Because of my anti-racist beliefs, they used the information they gathered to threaten me, my family, and my friends. In every harassing email and social media comment, they characterize the projects I participate in as "terrorist groups," describing me as a "leader" and member of an imaginary "shadowy mob of violent leftists" that they want to "do something serious about." Whether these conclusions are just shoddy investigative work or intentionally dishonest misrepresentations, their behavior should be concerning to anyone who believes in standing up against oppression.

I deactivated my social media when I learned that this was underway—not because I am ashamed of being associated with the struggle for a freer world, but because I want to protect my friends and social networks. Anyone who knows me knows it is no secret that I oppose all forms of bigotry and oppression. They did not target me specifically for anything in particular I have done, but because they are opposed to *all* anti-racist, feminist, and queer activism and they think that they can isolate and intimidate us one by one. This is why we need to stand by each other.

I want you to know about this in case you ever find yourself in the same situation. You are not alone. I hope this encourages you to think seriously about your personal online security and the security of your family members and friends.

Robert Bowers, the Pittsburgh synagogue shooter, publicly chatted with alt-right trolls who doxxed anti-racists. The stalking campaign against me shows that they are willing to manufacture falsehoods to put people in those crosshairs. The only way to protect ourselves is to keep showing up for each other. We must not let them intimidate us.

What Is Doxxing?

Doxxing means publishing a person's private information with the intention of exposing and intimidating them. This can result in physical, emotional, and economic harm to the target. It is intended to dissuade the target from action and to shame them for their ideas and values. It is important to take security seriously before you are doxxed—before you even have reason to fear that you could be doxxed. Often a doxxer will wait until they have gathered a lot of information before releasing it. It is possible that you are already being stalked and will not find out until it is too late.

Whether you are a well-known public activist or hardly involved at all, you should protect your social networks and other spheres of your life—even if you don't think you are doing anything that would warrant attention. Maintaining good practices protects your friends, family, and community. It is common for people to be included in right-wing conspiracy theories about "Antifa members" solely because they are queer or trans, "look like a leftist," play in bands, attend an event, or hang out in radical spaces. The information does not have to be correct or justified for someone to target you. All a harasser needs is one piece of information to begin to seek more details online.

Being aware of what information trails you leave online can protect you from law enforcement as well as stalkers. Now that state-imposed surveillance is increasingly sophisticated and livestreaming has become normal at protests, just wearing a mask is often not enough. In June 2020 in Philadelphia, investigators identified a woman starting with nothing more than a blurry photo of her. They followed a trail of breadcrumbs including an Etsy purchase, twitter accounts, and her professional work page. Customs and Border Protection have started to trawl public social media. Securing your online presence can make you feel more secure taking action offline.

An Ounce of Prevention Is Worth a Pound of Cure

There's no better time to start than now. After you have been doxxed, you may not be able to eliminate the information that is out there even if you try to get it taken down.

There are many different ways to approach this. Obviously, the best way to ensure that no one can find any information about you is to have nothing available—but some people can't eliminate their online presence, whether because of work, family, or other responsibilities. In some cases, there are strategic reasons to maintain some sort of online persona; for example, having a longstanding, believable but innocuous social media account may be helpful for non-citizens crossing the US border. Thankfully, there are ways to firewall distinct spheres of your life, curate a public profile if you need one, and adopt practices that can help you and your friends to feel empowered to continue taking action in your community. This process can be tedious. It will take time and energy. I recommend doing it together with friends, roommates, or family members to help through some of the difficult or boring aspects.

Maintaining Separate Spheres

If you cannot completely delete yourself from the internet, you can still preserve relative privacy by maintaining distinct spheres[1] of online activity and cleaning up forgotten or infrequently used accounts.

You likely have more than one online presence. This could include social networks, message boards, job sites, email accounts—anything you need to log into. Often in doxxing, information is triangulated from many different sources. One way to reduce the amount of information available to doxxers is to partition these spheres so they are not connected to each other. This is a highly individualized process; take some time to consider the following questions and map out your own online spheres.

[1] The concept of spheres was developed by the Smiling Faces Collective.

Do you spend your time on r/politics or the wall of a Facebook acquaintance debating? Do you frequently like or repost statuses from radical Instagram or Twitter accounts? Do you have images or personal information on job boards? Do you buy things on Etsy or eBay? Do any of your friends post pictures of you on their Instagram accounts? Do you have to promote yourself online for the line of work you are in? Do you connect with your co-workers, family members, and activist friends using the same account? Do you use parts of your real name or birthday for usernames or emails?

Each of these may not be a problem in and of itself, but together they can create links between different spheres of your life.

Ask yourself:

- How separate are each of these accounts/identities?
- What is public? What is private?
- What does public and private mean in the context of each site?
- What can be found by searching your legal name?
- Do you use the same username or email for multiple accounts? Do these cross over into distinct spheres of your life?Take a moment to think about the way in which all of these spheres overlap offline.
- Does your job allow you to be open about your politics?
- How public is your activism? Do you speak to reporters? Do you work at an infoshop?
- Do you filter some or all of your social media content from relatives?
- Are there any references to illegal or controversial activities in a given profile?

Here are a few examples of how your online presence can overlap across different sites:

Relatives

- How open is the relationship between you and your blood/legal relatives? If a stranger had information on just one person in this network, what could they discover about the others?

Politics

- Do you discuss or post about your political beliefs online? If so, on which platforms?

Friends and Community

- If you have social media, who are your friends? Your followers? In what ways do your online communities reflect your IRL communities?

Hobbies

- What hobbies do you have? Do you have friends and community through them? Are you a part of any internet communities dedicated to those hobbies?

Legal

- Who are you on paper? What names, phone numbers, and addresses are you tied to? Do any of your accounts include this information? Do any other sites (probably without your permission)?

Career

- Does your job involve an online presence, website, or social media account? Would there be a problem if your politics overlapped with your career? Or is your career in some way tied to your political identity?

Take time to consider where you overlap, what your online goals are, and where you can separate these spheres.

Tactics

Let's talk about how to discover what information is available about you, how to identify and eliminate trails, and what online resources exist to remove them.

Begin with what is publicly available. Google yourself and make a list of all of your social media accounts. Delete old accounts for things you no longer use. This is also a good time to download a password manager like 1Password or LastPass to assist you in managing unique usernames, emails, and passwords.

Delete off Snoop Sites/Data Brokers

Find out what information people can find out about you simply using a search engine. Search for yourself on DuckDuckGo and Google. Try doing this search in incognito mode. Try different versions of your name, with and with out your middle name and in quotation marks. You could set Google Alerts to send you emails when your name is published on the internet. This will give you a sense of how much data about you is available online to people who are not in your network.

After this initial search, have a look at all of the data broker sites that profit on trading in personal data. I also encourage you to remove your closest family members at the same time. This process can be arduous; these sites try to make it as difficult as possible to delete information about yourself. There are some things you can't remove yourself from—for example, if you recently registered to vote and still live at that address. (This is another reason some people choose not to vote.)

The most trafficked host sites includee: Been-verified, CheckPeople, Instant Checkmate, Intelius, PeekYou, PeopleFinders, PeopleSmart, Pipl, PrivateEye, PublicRecords360, Radaris, Spokeo, USA People Search, TruthFinder.com, Nuwber, OneRep, and FamilyTreeNow. I recommend starting with these by searching each one on this website, which has a guide for opting

out of virtually every data broker. If you have more money than time, you can pay for a service called Just Delete Me to have your information removed, but I usually only recommend this service if you have already been doxxed.

Delete Old Accounts

When you search yourself in a online search engine, you may also find old accounts. It can be good to do a reverse search using all of the old user names and screen names you can remember. Accounts you have not used in a long time can make you vulnerable because if they are using an older password, they can try that account's technical support to get more data about you that they can try to use for other accounts. Download any material of sentimental value to you and permanently close all the accounts you no longer use. These can be full of clues about your life.

First, go to namechk.com, which searches over hundreds of platforms for specific usernames, and search all the possible usernames and emails you have used. This will tell you what platforms have accounts using that handle.

Second, go to backgroundchecks.org/justdeleteme and type in the website domain. This website archives a huge array of existing websites, categorizes how easy or difficult they make it to delete an account, and provides the link to the "delete profile" page for each respective site.

Haveibeenpwned.com will help you find out if there are any data breaches involving any accounts you hold. If there are, take immediate action to change passwords.

Change Usernames, Email Addresses, and Passwords

The easiest way for someone to find more information about you is to search your name, aliases, and usernames. To keep your spheres of internet activity separate, *always* use a new username when you create an account. If you have a professional website for work and must use you legal name, make sure the email you use for that account is used solely for that purpose. You may have to have a handful of email accounts and usernames. I have one for all of my medical and governmental accounts, one for my online shopping, one for my political life, and one for my social media, another for dating sites, and so on. I use aliases and false information for all the websites that represent me or display photos of me.

A password manager is a great help for this, as it will store logins for all of your accounts. I recommend LastPass, which you can download for your phone and web browser. It might be tempting to leave yourself permanently signed in, but always make sure to sign out when you are done using it. First, so you don't forget the master password—and also to ensure that even if someone manages to gain access to your phone or computer, they can't access all your personal data. Take this time to create new emails and change usernames for all of the accounts you aren't going to delete. You can easily create new emails using Protonmail. Both 1Password and LastPass can help generate random string passwords, which are the most secure.

Curate What Is Available and Change Your Privacy Settings

Once you have eliminated all your loose ends, take a look at what you chose to retain and what can be found there. If you keep any social media accounts, go through your profile and note

what people can find out about you. You can choose from a range of strategies regarding how to approach this, depending on how cautious you want to be and how certain are that it is possible to keep your different spheres of internet activity distinct.

Some of your options include:

- Deleting all photos of yourself, your pets, your car, your mailbox, tattoos, and anything else that includes unnecessary identifying information—especially your public profile picture.
- Eliminating or falsifying any personal details in your profile—give an inaccurate birthday or no birthday at all, choose random answers for your hometown, schools you have attended, and other information.
- Deleting questionable followers and friends. If you change all of your social media settings to private and you feel confident about your followers list, there may be less reason to hide your face. I still recommend keeping details about your location and intimate personal life offline. Remember, you are only as safe as the most open person in your life. If you choose to be more public, keep your friends and family separate, do not post pictures of them or their personal information without their informed consent, and remember that social connections are visible through social networking and data collection websites.

The Coach from Crash Override Network is a helpful step-by-step guide that links you directly to the privacy settings page for many commonly used social networks. Click "Let's Get Started" and "Strengthen the security of my online accounts so people can't break into them as easily," and follow their guides for all the top social media companies. This guide can also help with other aspects of online security, so after you've done that, I recommend finishing the Coach helper and checking out what other resources they offer.

When you think you are done, have a friend try to create a profile based on what information they can find about you while pretending to be a "doxxer" to see if anything you didn't think of slipped through the cracks. It may be important to periodically check in on what can be found by searching your name every few months.

If You Have Been Doxxed

We do not recommend approaching the police when you are doxxed (or ever). The police may use the information you give them about the harassers, but they will also use the information they get about you and other individuals and groups you may have been publicly associated with. Once that is on file, it's permanently in their hands, and there's no guarantee they won't use it to target you or others with state repression.

If you chose to involve the police, please be transparent and do not ask any radical groups to support you. Be sure to inform any groups that you are connected with of your decision. Usually, the police will do nothing or make the situation much worse. The idea of thiis guide is to provide you with alternatives based in community support and empowerment.

Should I Go Public?

Short answer: Do not immediately react publicly. Take time to secure yourself and alert your networks privately before reacting publicly.

Your first impulse may be to alert as many people as you can immediately with a public announcement or to shut everything down. Going public in this way can provide you with immediate support if you have a sympathetic audience, but it carries the risk of increased aggression from harassers. There are good arguments for being cautious with information at the beginning. The most important thing to do first is to take steps to protect yourself and your networks against further harm.

Immediate announcements can complicate your security efforts. Whether or not the information posted about you is accurate, no one is likely to use it to cause you any serious harm without first confirming at least some of it. Posting on a social media account confirming your doxx immediately confirms that the information about you is accurate; it also indicates that you have seen where it was posted and suggests that you are terrified. This furthers the goals of your harassers. They want to intimidate and isolate you. Do not confirm or deny any of the information they have dug up about you, regardless of whether it is false or embarrassing. They are seeking a reaction. If you let them know that what they have posted is incorrect, they may conclude that they are on the right track and they just need to keep digging. Sometimes, one of the most effective initial public responses is no response at all—don't make any major changes to your posting habits or show any fear. This can send the message that your doxxer missed the mark, and that the attack was a failure.

After you have had time to process your feelings and secure your position, it may be strategic to go public and perhaps to band together with other people who are in a similar situation. You may be able to leverage the public outrage over white supremacists to create a campaign to dissuade further doxxing—for example, make a funding drive with pledges to give money for every harassing email you or others in your community receive! Since your harassers want to isolate you, public support like this may dissuade further intimidation. Try to be creative, resilient, and strategic. Be careful not to endanger anyone else in this process.

When making public statements, if you posture or brag about your abilities, your ability to employ violence, weapons with which you can defend yourself, or overstate your ferociousness, you may bite off more than you can chew. It is generally not a good idea to misrepresent yourself. Talking directly or indirectly to the harassers does not usually improve matters. I recommend making a positive statement asserting your ethics and beliefs, describing how your identity or your ideals have made you a target but maintaining that while these campaigns of harassment are intended to make you cower, you will not do so, because you have no reason to hide your politics. Avoid talking about specific actions or groups, whether or not you are involved with them.

Immediately after Being Doxxed

1. **Don't panic.** Call a close friend to come over and help.

2. **Create an incident log** and keep records for both online and offline provocations. This is crucial to identifying the patterns of the attacks. It can be useful to compare these with

other organizers in order to identify larger patterns so as to identify your opponents and their organizations.

3. **Alert your friends, family, and sensitive political networks privately.** Task a few friends that you trust with your personal information to help report social media and blog posts that doxx you, identifying them as harassment. Do so repeatedly. Some platforms lack policies that will protect you, even if these posts include accurate personal information, even if they put you in danger. Sometimes, doxxers will use your photos and information to make imposter accounts. It is usually easier to report these as fakes; try to do so quickly in order to prevent them from obtaining more information from your networks by posing as you. You, your family, and your employer may begin to receive threatening or harassing phone calls. Let them know what is happening as quickly as you can and instruct them not to engage with the harassers.

4. **Shut down the flow of information.** If you are reading this section and have not done the preventative care section, begin that process. Download a password manager like 1Password or LastPass and change all of your passwords immediately. You can also pay for a service called Delete Me that will take much of your online footprint off of snoop sites that harvest and display personal information. This service will take care of the information aggregated by the data brokers but not any social media, web accounts, news articles, or arrest records you may have, those will have to be handled on your own. It is important to balance the hemorrhage of information, while also not alerting your harassers that the dox was effective or on target. Try to shore up your social media accounts by making friends lists and information private in order to protect your networks until you are sure that they don't offer vulnerable personal information to those willing to dig for it. How you react publicly is a very delicate situation and should be handled carefully throughout this process.

5. **Set up a safety plan.** Recruit friends and family to support you. Let them know what is going on; doxxing can be traumatic and you need to prioritize your mental and physical health so that you can work through these attacks. These conversations can be difficult—especially if they do not understand the nuances of this political moment, if it's the first time they are hearing about a particular flavor of hate group, or if your relationships are strained due to political or personal differences. If you don't feel up to it, you could ask a friend who has a good understanding of the situation to have the more difficult conversations for you.

If your home address is included in the doxx, find somewhere new you can stay if you are able. If you can't leave your home, invite friends or a local security group to stay with you. Make a "go bag" with everything you will need if you have to pack up and go with little notice.

Evaluating Threats

If you don't feel you are at any great risk, especially if your doxx is comprised of freely-available information or is just sent directly to you in an effort to unnerve you, you may feel fine dismissing it as a cheap intimidation tactic, blocking and reporting the harasser, and moving on. It may just

be a matter of someone trying to get a rise out of you. However, if your doxx includes sensitive personal information, especially details that are not easy to obtain with simple detective work, or it appears in a public forum where people distribute information in hopes that others will act on it, you may want to take further precautions. This is especially true if you are already part of a targeted group or demographic.

When you learn that you have been doxxed, it's important to establish which information could translate into credible threats. Often, doxxing is a precursor to more intrusive offline harassment, or is connected with threats to act on the information. This could be anything from threatening phone calls to family or workplaces to pointed death threats or a SWAT call.

It is sometimes difficult to determine what makes a threat "credible." The most common tactic of ordinary doxxers is to send creepy or intimidating messages wherever they think they can reach you—social media, email, and to family members, and the like. They will often imply that they have more information than they really do; it's common for them to say that they have provided this information to local law enforcement. Their goal is to intimidate you out of acting; often, whatever information they post publically is all that they have.

Your employer may receive calls demanding that they fire you. Thus far, it is rare that the targets of doxxing have been physically attacked, but it *has happened,* and it is possible that those who doxx you may make efforts to get your information into the hands of people who are not acting rationally or ethically. It is important to be cautious, but don't panic or immerse yourself in anxiety.

Ask yourself:

- Is the information accurate? Do they have your home, work, or family address? Do they know places you hang out? Who you are friends with?
- Are you at risk of losing your job if they find out any of this information about you?
- Do you know where the harassers live? Are they close to your physical community or just online trolls on a decentralized forum? Do you have reason to believe law enforcement will be interested in this information? Is the information being shared from local right-wing news sources, putting your face in front of a multitude of hostile strangers who now have your information?
- Do they have embarrassing or private photos of you?
- Is there information tying you to criminal activity that could get you arrested?

Solutions

Here are some things you can do in response to the dangers that can arise from being doxxed:

- Create a self-defense plan, sign up for self-defense classes, contact a local community defense group.
- Inform the people and groups that are named in the doxx—workplace, comrades, roommates, family.

- Talk through your fears with people you trust.
- Contact people who have been through this before for advice.
- Arrange to have a lawyer available if you are worried that the information about you may be of interest to state actors.
- Connect with a local anti-fascist group—they may be able to help identify the doxxers, if the latter are posting from fake account.

Having Conversations with Jobs and Family

This conversation can be very difficult, especially if your relationship with your family is strained. Have a cool-headed friend on call to help mediate or support you afterwards if necessary.

Think about how often you are willing to be vulnerable with your family and how much opportunity you will have in the future to follow up on the conversation. If it's necessary to speak to family members but you feel like you will only get one chance, you can rehearse with a friend and prepare for their reactions. If you have an ongoing, conversational, trusting relationship, you can explain the situation to them in a series of smaller conversations, instead of one long sit-down. Evaluate how much time and how much attention you will have.

It has always helped me to frame this as "having a stalker" to people who I do not want to have a political conversation with—that may suffice to explain the severity of the situation and why you need privacy. But it can be worth the effort to be honest about what's going on. This can help build stronger relationships and demystify this common occurrence, while encouraging others who may not have considered that it could happen to them or someone they know to take online privacy seriously. Most people will respond with fear and sympathy, though sometimes they will suggest or even insist that you call the police.

There is no one-size-fits-all approach. In my case, I had to compel my conservative mother to promise that she would not involve the police. I did so by appealing to my right to personal safety and my autonomy as the victim in the situation, asking her to respect my wishes and reminding her that the police can do very little to respond to targeted harassment like this—and all that calling them would do would be to open me up to their scrutiny, since I was being accused of criminal activity. Such conversations can be very difficult, but they are often necessary. Remind your friends and family not to react or respond to any phone calls, emails, or social media requests.

Things to remember when talking to your friends and family:

- The harassers' goal is to strain your relationships and ruin your life. Do not let them succeed at doing this. Tell your family that the best way to support you is to refuse to give in to their tactics.
- Don't throw anarchists and anti-fascists under the bus or claim that you are being targeted for no reason. This will not serve you if reasons emerge—and it will only delegitimize and further endanger those who can't distance themselves from anarchist politics.
- Do not let anyone blame you for what is happening, whether for the politics you adhere to or your perceived irresponsibility for getting yourself "into this situation." Fighting for

a better world involves challenges. If anything, it is to your credit that you have provoked this response by your efforts.

- Suggest concrete ways you can help them understand the situation and protect themselves. Send them this article or a list of resources; offer to help them lock down their social media if they are not tech savvy.
- Talk through what they can prepare for—harassing phone calls, emails, perhaps the neighbors will receive messages about you. Prepare them for worst-case scenario, but emphasize that it is unlikely.
- Be clear about what you need from them.

Living Your Life, Moving Forward

Take a deep breath. Do not blame yourself. Emotionally this can be deeply disturbing and disruptive, adding a layer of acute stress to your life. There may be people out there who know what you look like and you will have no idea who they are. Sometimes information from doxxes becomes a permanent part of the internet if you name is googled; this can affect your job prospects. Sometimes nothing comes from the attention—but there is always the possibility that someone will try to pick up where the last doxxer left off.

Until you are sure that your time in the spotlight is over, you may have to alter some aspects of your life. Ask yourself, "What kind of life do I want to live? How can I manage my anxiety? Are there ways I can embrace being a more public figure? How can I feel secure in taking risks and being active again?" Especially as political tensions intensify, it may be important to take more extreme safety measures.

Here are some of the measures you might choose to employ:

- Do not let anyone photograph you unless you trust them to handle the images the way you need them to. This can create some awkward conversations, especially at family events or in professional situations. Be aware of who appears in photos with you; inform them that appearing in a photo with you may attract unwanted attention. It can be helpful to rehearse the conversations you may need to have.
- Install trail cameras at your house.
- Keep logs of all harassment you experience.
- If you move, do not update your address. Do not register to vote, as this makes your address publicly available. Try to hold on to your old driver's license or ID and receive mail at a post office box. Consider when to use a real address and when to use a fake one or omit your address altogether when you sign up for things online or in person.
- Use pseudonyms online and in person if need be. Don't use the same one over and over.
- When you go to actions, especially if you don't mask up, be aware what groups, places, or individuals could be implicated by being seen or photographed in your vicinity.

- Invest time in self-defense classes. This can include weapons training, but should include defensive and disarming training.
- See a therapist to work through any trauma you have experienced.
- Help your friends and family understand the importance of online security.
- Have frank conversations with people outside your circles of political affinity. You may be surprised at how much empathy they express.

No matter how hard the people targeting you try make you feel isolated, you are not in this alone. As a community, we must protect each other and our online networks from harassment, imprisonment, political violence, and intimidation. Together, **we can do this.**

CrimethInc.

Doxcare

Prevention and Aftercare for Those Targeted by Doxxing and Political Harassment

August 26, 2020

Retrieved on 29th October 2020 from crimethinc.com

usa.anarchistlibraries.net