Doxxing: Tips To Protect Yourself Online & How to Minimize Harm

Daly Barnett ⋮ 9-11 minutes ⋮ 12/16/2020

“Doxxing” is an eerie, cyber-sounding term that gets thrown around more and more these days, but what exactly does it mean? Simply put, it’s when a person or other entity exposes information about you, publicly available or secret, for the purpose of causing harm. It might be information you intended to keep secret, like your personal address or legal name. Often it is publicly available data that can be readily found online with just a bit of digging, like your phone number or workplace address.

By itself, being doxxed can be dangerous, as it may reveal information about you that could harm you if it were publicly known. More often it is used to escalate to greater harm such as mass online harassment, in-person violence, or targeting other members of your community. Your political beliefs or status as a member of a marginalized community can amplify these threats.

Although you aren’t always faced with the option, taking control of your data and considering precautionary steps to advance your personal security are best done before you’re threatened with a potential doxxing. Privacy does not work retroactively. A great place to start is to develop your personal threat model. After you’ve done that, you can take specific measures to advance your data hygiene.

First Steps To Protect Yourself

First: **Take a look at the information that is already publicly available about you online.** This is as simple as opening up a search engine and entering your name/nickname/handle/avatar and seeing what comes up. It’s common to be overwhelmed by what you find: there can be much more data about you than you expected readily available online to anyone that cares to do a little digging. Remind yourself that this is normal, and that you are on your way to reducing that information and taking the necessary steps to protecting yourself. Take note of any pieces that strike you as high priority to deal with. Keep track both of what the information is and where you found it.

Second: **Identify who you can trust with your secrets.** Friends, family, chosen family? If you are fearful of being doxxed, you’ll want to speak with these people directly. Not only because they can be implicated in a doxxing incident, but also because there is strength in your community. These trusted folks can help you plan how to prevent an incident from happening, and also what to do in the event of one (more on that below). Keep in mind that this list will change over time. It’s natural for relationships to ebb and flow, and so will the amount of trust you ascribe them with. Set a reminder for yourself to check in on this list once a year or so.

Set some data sharing community ground rules such as asking for permission before taking/posting photos, refraining from geotagging those photos, or using code words to imply something else that only trusted people know. These are all examples of steps you can take to strengthen your social community’s security posture.

Third: **Read up on the policies your online accounts have.** Most major social media platforms and other popular web apps have policies and procedures in place that protect users against doxxing and allow them to report any violations. Review that information and note how to get in contact with their support teams.

With these non-technical steps out of the way, you can begin to think about the more technical steps you can take: both as precautionary steps ahead of time, and if you have to respond to a doxxing incident.

Minimizing Your Publicly Available Data

The most obvious protective measure you can take to prevent being doxxed is to reduce the amount of material there is about you online.

Data brokers are companies that subsist entirely off collecting this data, repackaging it, and selling to the highest bidders. The information they gather is often from public records and online trackers, and augmented by commercial transactional data. It is a parasitic, rotten industry that survives by invading the privacy of everyday people online. Due to public pressure, many of these companies offer ways for users to opt out of their data being shared. We recommend starting with White Pages, Instant Check Mate, Acxiom, Intelius, and Spokeo. Also take a look at these other helpful guides on how to remove yourself from people-finding services and data brokerage companies.

For a more thorough—though more costly—approach, several professional services like DeleteMe or Privacy Duck claim to help minimize the data available about you online from these data brokers and similar sources. Beware that data brokers work by *continually* scraping public records and repopulating their data, and so services like these can require ongoing subscriptions to be most effective. They also cannot (and do not) promise comprehensive data minimization across all possible sources. Users should conduct their own research and consider whether these kinds of services can successfully target the data sources you are most concerned about.

Safe Browsing

Sometimes software behaving as expected can lead to our secrets ending up in places they shouldn't. For example, suggested friends lists can sometimes "out" you to people despite your having multiple accounts for the very purpose of keeping parts of your life separate.

Most other common examples are the fault of user tracking, which you have the power to minimize. If that's a concern you want to address, here are some steps you can take:

Check how "fingerprintable" your browser is with our tool Cover Your Tracks. This will give you an idea of how capable those very trackers are of uniquely identifying you and your actions online. We also recommend **adding our install-and-forget tracker blocking tool, Privacy Badger**, which is designed to silently halt those trackers and let you browse in peace.

From there, you can begin to assess the rest of your personal data hygiene online. To protect your account security, are you **using strong unique passwords and multi-factor authentication** on each of your accounts? Both of these steps will do wonders in preventing your account from being maliciously hijacked.

As you consider each of the accounts you use online, we highly recommend taking a moment with each to **look at what information you share**. Do you share with them the bare minimum so that you can continue to use their software, or are you giving more than what's necessary? Instead of listing your mother's maiden name, prom date, or pet's name in response to security questions, consider inputting a random passphrase instead and keeping it in your password manager. And instead of handing over your phone number—a common bit of information behind account compromise and unwanted identification—consider what the phone number will be used for, whether Facebook or Twitter or whomever actually needs it, and if you can substitute your mobile number for something less individually identifying like a Google Voice number. Remaining mindful of what information you're sharing, as well as when and where you're sharing it will do wonders for your data hygiene.

Incident Response Plan

Being doxxed is a stressful, scary thing to endure. In the event of it happening, the last thing you'll want to be doing is scrambling at the last minute to figure out how to respond. Having a ready-made plan in place will do wonders for you. Here are some suggestions on where to start:

Decide which accounts to lock or temporarily deactivate if you're being doxxed. Make a list. It will help to walk through the process of deactivating/locking the account for each so that you can take note of any special steps that they may require.

Have a spreadsheet template handy to record incidents as they happen. You'll want to have fields ready to mark when something took place, who it appears to be from, where it's happening, and any details about what happened. Making this log will be incredibly useful: it can help you identify where the weakness is in your personal data security, as well as provide a detailed log of events that you could pass along to others.

Care for Yourself, Care for Others

Finally, you'll want to include people from your trusted networks to help you in this process. Knowing you've got friends to support you if you're being doxxed will not only ease the burden of stress and labor, but can also alert them to how they might be implicated. We recommend going over this whole process with a trusted friend. Knowing they're available to take over during a crisis will ease your mind. Reciprocating that help for them builds community trust.

Data hygiene is a form of community self-care. Establishing data hygiene standards with your close network can be a way of caring for yourself, and them. After all, an incident on one node of a network could compromise other nodes on the same network. Caring for your own data hygiene will in part strengthen your community's, and vice versa.

Join EFF Lists