Prevention:

1. Remove your personal information from as many sites as possible.
2. Make your social media accounts as private as possible.
3. Use strong, unique passwords & two-factor authentication.

Removing personal information: Google yourself and see what comes up. You'll often be surprised by the amount of your personal information online. It's better to know this now than be surprised in the event of a doxxing situation.

- Most of this information is collected and sold by data brokers. It's relatively easy, but time-consuming, to opt-out of these sites. They all have a form where you submit a request to have your listing removed. You can either follow a worksheet that goes through all of the data brokers or pay a private service to remove the listings for you. Remember, you don't have to do this all at once. Every step you take is good, and increases your safety online. Break it down into manageable chunks.
- Your personal information also exists outside of data brokers. Your employer or an organization you're a member of might have your full name and picture posted on their website. See what comes up, and determine how comfortable you are with that information being easily accessible. It's worth asking to see if you can have information removed or in less detail online — people are generally really willing to work with you and help out, no questions asked.

Protect your social media: Review your privacy settings on all your accounts and make sure you're only sharing with the audiences you intend to share with. Also, make sure only people who are your followers/friends can contact your accounts. Adjust your settings as needed. You also want to make sure your social media accounts aren't able to be found via Google if someone searches your name — this is usually a setting you can turn off. You don't have to completely cut out public social media, but it's worth thinking about if you really want your posts to be so easily avaliable in the case of a doxxing incident. It's also worth going through old posts and deleting anything that has too much identifying information, be that information in the post itself or in your tagged location — use the "on this day" feature to go through your old posts in a manageable way. Remember, just like with your personal information, this isn't something you need to tackle all at once. Every improvement you make is good and will make you safer.

Keep your accounts secure: Make sure you're using strong, unique passwords for every site. Check out haveibeenpwned.com to see if your email or passwords have been exposed on public breach lists. If so, change that password, and any other instances where you used that password. Any easy way to keep track of your passwords and ensure they're all unique is by using a password manager like Dashlane, 1Password, or Bitwarden. Set aside some time to go through all of your accounts and change each password, saving it in the password manager — again, each one you do will make you safer. As you change your passwords, set up Two-Factor Authentication (2FA) on all the accounts that support it. 2FA means that instead of being able to sign in with just a password, you also have to have a physical object (your phone, a security app

or key) to access the account. This means even if someone gets your password, they still won't be able to log into your account. Most commonly, this involves sending a security code to your phone that you enter at log-in, but you can also use an app like Google Authenticator as well.

Response:

You've been doxxed — now what?

First, take a deep breath. Hopefully, you've already gone through the steps in the prevention section. If not, start there.

Next, we want to think about escalation paths — a bad actor will always take the easiest path. If the effort it takes to harass you will take an additional 5 minutes of research, most harassers will move on to the next target and leave you alone. Now, if you're a defendant in a high-profile case or the focus of particular attention by the right, they might be willing to invest more time, but as the seriousness of a threat escalates, the likelihood of it happening generally decreases. By interrupting their escalation paths, we short circuit the attack and make sure it can't turn into anything bigger.

Common escalation paths for harassment are:

- Finding your password on a breach list and attempting to use it
    - Strong, unique passwords and 2FA will remove this path
- Finding your home address or phone number on a people finder site
    - Removing your listings from data brokers, manually or using a service, will remove this path
- Finding information about you from social media and harassing you there
    - Making sure you have strong privacy settings and blocking harassers will remove this path
    - If your account is public, lock it down.
    - You can change your name and profile picture to make your account less recognizable to harassers, too.
    - Block pre-emptively — blocking the accounts of known right-wing commentators will prevent them from being able to draw immediate attention to your account. They still might be able to post screenshots or whatever other information they have, but you're denying them engagement with your posts and sending people directly to your account

Here are some more tips:

- **Tell people what you're going through**. The point of harassment is to make you feel isolated and alone — don't let them win! Make sure your close friends and loved ones know what you're going through so they can support you. You'll also want to let people know so they can be wary of fake or hostile communications. People might try to impersonate you in order to embarrass you, gather additional information, or try to scam. Decide upon an reliable communication method (phone calls, IG message, etc) —

something unique so they know it's you and not an imposter. If you have children, check in with your kids' school or daycare — they have already rigorous rules in place for who can be on campus or pick up kids, but hearing those rules again directly and asking them to keep an eye out can give you real peace of mind.

- **Don't be afraid to ask for help.** This can be really overwhelming! Delegate tasks like screenshotting harassment or explaining phishing to your parents to a loved one. You can't do this all by yourself. Let people support you — they want to help!
- **Be especially wary of phishing** — usually emails, but can be voicemails or social media messages that impersonate a trusted sender to try and get you to click on malicious links or disclose personal information.
- **Document before you delete or block.** If comments or messages are crossing the line, screenshot them. If you decide that you want to pursue a legal response down the line, you'll need proof of these comments. Download or screenshot the content in question so you have it later on. Then you can delete the content and block and report the sender.

Resources:

Speak Up & Stay Safe(r): A Guide to Protecting Yourself From Online Harassment - free comprehensive guide
A DIY Guide to Feminist Cybersecurity - free comprehensive guide
Delete Me - paid service ($10/month) which will constantly search and remove you from data broker listings online. We highly recommend this and use it personally.
Big Ass Data Broker Opt-Out List - free comprehensive guide for if you don't want to use a paid service to do data broker removals