INFORMATION ECOLOGY Doxxing Prevention Resources

Doxxing is when someone maliciously posts your personal information on the internet, generally for the purpose of harassing you and encouraging others to do so. Here are some basic steps to take to reduce your risk of being doxxed. (There are tons of guides out there with more detailed steps; this is intended to be brief and high-level.)

Be aware that as of early 2025, political opponents and law enforcement are increasingly sharing information. Having personal information exposed online, especially if you are not a US citizen and/or are organizing for bodily autonomy, immigrant rights, and/or free Palestine, can increase your risk of targeting by law enforcement and/or immigration authorities. This makes the Other Preparedness Steps to Consider section below even more important.

This resource is focused on prevention. If you are currently being doxxed, log everything and get support! Here are some additional resources.

SCRUB YOUR PERSONAL INFORMATION FROM THE INTERNET

Data brokers and people-search websites can make your information easy to find on the web. You can work to remove it yourself, but it's a tedious and ongoing process. Instead, you may want to use a service to do this instead. This article from Consumer Reports covers both options.

Doxxers may also use face recognition tools to identify who people are via images (for example, pictures taken at protests). PimEyes and FaceCheck are two of the most popular; it's recommended to opt out (see https://pimeyes.com/en/opt-out-request-form and https://facecheck.id/Face-Search/RemoveMyPhotos).

INFORMATION ECOLOGY

SET YOUR SOCIAL MEDIA ACCOUNTS TO PRIVATE

Limit sharing and who can follow you to people you know and trust. Each social media platform has its own options you can control and some give you more power than others. Search for each platform you use along with "privacy settings" to learn more about what you can do and how. (Both the links and the steps can change, so we're not going into detail here.)

Also, people who want to dox you will often first try to collect information from social media. Don't accept connection requests from people you don't know!

SET UP SOME ALERTS

Set up a Google alert on your name so you will get emails when you are mentioned on web pages that Google indexes. You may also want to set up alerts on services that monitor social media (here are two lists of such tools); these services are generally used by businesses for marketing purposes but you can use them to see if people are talking about you and what they are saying, which will help you see if your information is circulating.

BE ON GUARD AGAINST SOCIAL ENGINEERING

Generally, any unexpected messages should be looked at with suspicion, especially ones that ask you to do something (this is just as true on text, WhatsApp, Instagram direct message, etc., as it is for email). Even if a message seems like it's coming from someone you know, if they are asking you for anything out of the ordinary or have sent an unexpected or unusual link or attachment, check with them through a method that's different from the original method to make sure it's really them.

Never click on links or attachments in messages from senders you don't know (or who you can't confirm are who they say they are if you do know them). These links will generally send you to a page that looks like a login page to your bank, Google, etc; if you "sign in," you are actually revealing your username and password to the sender. Attachments are generally viruses or malware that will install themselves on your device in order to hijack computing resources or exfiltrate data.

Do you need help with any of your technology and information systems problems?
Get in touch!

https://iecology.org * 510-479-9779 * info@iecology.org

INFORMATION ECOLOGY

BE ON GUARD AGAINST INVASIVE SOFTWARE

In addition, the proliferation of mobile apps, browser extensions, and other no- and low-cost programs has caused numerous security problems, as software that appears to have good intentions (like antivirus scanning) or beneficial features (use your phone as a flashlight!) may be masking malicious activities in the background.

As much as possible, avoid software that hasn't been created by a company you trust. Beyond that, in most browsers and mobile devices, an application will ask for certain permissions at installation; be sure to check these to make sure they at least vaguely reflect what is expected. For example, if a flashlight app asks for permissions to your contacts or to make phone calls, you probably don't want to install it. Be especially cautious about granting permissions such as access to your calls, contacts, camera, microphone, location services, or entire storage.

USE STRONG PASSWORDS AND TWO-STEP VERIFICATION ON ALL YOUR ACCOUNTS

Passwords

Your passwords should be long, unique (i.e., you don't use them for more than one account), not written down anywhere except a password manager app, and private (i.e., don't tell anyone your password for any reason). You will generally need at least a few that are also memorable (because you can't access your password manager from outside your device and your password manager).

There are many ways to generate strong passwords. Security In a Box has a good guide and most password managers will also make a random password for you, as will other available software for that specific purpose. Diceware is a fun and effective method for creating random yet memorable passwords using everyday objects and a word list. One other great way to make a strong password is to come up with a silly sentence that no one's ever said before and use the first letter or two of each word as your password, mixing in other types of characters.

Two-step verification

Two-step verification means that in order to log in to your account, you use something you know (your password) and something you have. While not every

Do you need help with any of your technology and information systems problems?
Get in touch!

service you have an account on will support two-step verification (sometimes called two-factor authentication (2FA) or multifactor authentication (MFA), most will.

Two-step verification adds a layer of protection to your accounts so that it is much harder to take them over. It is especially important to use two-factor authentication on accounts that grant a lot of access to your devices or files. Such accounts include those that allow you to push software installs to devices (such as Apple IDs or Google Play accounts) or to reset passwords for other accounts (any account you use as a recovery email for other services, for example).

Common recommended second factors are authentication apps and physical keys. Many services also offer a text message (SMS) option, but texts can be redirected and intercepted, so SMS verification is less secure than an app or physical key.

See more information on choosing a second factor in this clear and handy guide from global digital rights org Access Now.

OTHER PREPAREDNESS STEPS TO CONSIDER

If you are at high risk for doxxing, you may want to also prepare yourself with the following items:

- Make a doxxing response plan (you will want to keep a log of incidents, and document everything (date, time, URL, screenshot); report the doxxing; ask others to report it as well; you may also want to enlist others to do your monitoring for you to minimize the impact of the harassment on you)
- Make a personal safety plan, including for emotional support
- Seek advice from an immigration attorney if you are at risk of deportation
- Make an emergency plan for yourself and your family in case you are detained (e.g., who will care for children and pets)

Do you need help with any of your technology and information systems problems? Get in touch!