Self-Doxing Guide

Summary: This guide contains tips and resources for exploring open source intelligence on oneself to prevent malicious actors from finding and using this information for publishing, blackmailing or other forms of harassment.

Table of Contents

Edit me

Please consider the date when this article was last updated by looking at the bottom right corner of the page when evaluating the accuracy and security of the following guide.

Access Now Digital Security Helpline

Self-Doxing Guide

The threat

Doxing (also "doxxing", or "d0xing", a word derived from "documents", or "docs") consists in tracing and gathering information about someone using sources that are freely available on the internet (called OSINT, or Open Source INTelligence).

Doxing is premised on the idea that "The more you know about your target, the easier it will be to find their flaws". A malicious actor may use this method to identify valuable information about their target. Once they have found sensitive information, they may publish this information for defamation, blackmail the target person, or use it for other goals.

Self-Doxing to Prevent Doxing

Harassers and stalkers use several tools and techniques to gather information about their targets, but since these tools and techniques are mostly public and easy to use, we can also use them ourselves, on ourselves, as a preventative measure. "Self-doxing" can help us make informed decisions about what we share online, and how. (Of course, these same instruments can also be used to learn more than is immediately obvious about someone we have met online before we give them our full trust - for example to decide if we want to admit them to a private mailing list or group on social networking platforms.)

Methods used for doxing (and self-doxing!) include exploring archives, yellow pages, phone directories and other publicly available information; querying common search engines like Google or DuckDuckGo, looking for a person's profile in specific services; searching for information in public forums and mailing lists; or looking for images that the person has shared (and for instance may have also published in another, more personal, account). But it can also simply consist in looking up the public information on the owner of a website, using the personal mobile number published on the website or through a simple "whois search" (see below, in the "Search engines and more" section).

Warning: when practicing self-doxing, there is a risk of getting exposed to results that you may find disturbing. If you think you may need support, make sure you have close friends around when you do your research.

Before we start exploring these web services and looking for our digital self, it's a good idea to use anonymisation tools like the Tor Browser.

What to search for

To decide what to search for, you should try to understand what activities expose you to a higher risk of being attacked by trolls or other malicious actors. Why would someone want to spend hours of their time to track information on you in the internet?

This kind of attacks often affects minorities or people who support controversial opinions online, and the attack starts from the information that the malicious actor will find immediately available - like the nickname and profile used by the target in the platform where the attack has started, or the pictures the target has published in their page.

So if you think that someone might want to harm you by looking for personal information on you, start asking yourself how they got to know you. If you use your name and surname or a picture of your face on the platform where they learned about your existence, then this is what they will start from, and what you should start from for your self-doxing exercise.

If, on the other hand, a potential attacker knows you by a pseudonym (like the nickname or handle you use on that platform), your search efforts should focus on any connection that there might be between that pseudonym and your physical life (your name and surname, the place where you work, your home address, etc.).

If you are using a unique handle in the platform where your sensitive activity is happening, and have never used it for anything else, some traces might still be public, for example your IP address or your geolocation data. Check the properties of the pictures you've uploaded and the posts you've published: do they contain any identifying details, like your IP address or your location? If so, you might want to edit them so as to delete any sensitive information they may contain. Read more on how to control the information you share online in this guide on secure identity management.

Search engines and more

Once you have identified all the names and nicknames you want to look for, as well as pictures and other personal data (web domains you own, birth date, city where you live, etc.) you may have posted in your most exposed online profiles and web pages, you can start your search.

What follows is a list of search engines and other online services that you can use.

When you do your search, use a different browser than usual so that you aren't logged into your online accounts. In alternative, you can delete the history and cookies, and clear the cache.

- The most obvious place to start a search is **Google**. Before you start your search there, please note that on your usual browser Google may give you customized results that might not match with what an adversary would find. It's better to use a different browser to do this search (for example if you usually use Firefox, use Chrome for this search, or, even better, the Tor Browser).
  - Remember that if you are looking for more than one word, like your name and surname, you can refine your search by putting quotation marks (") around the words, as in: "Name Surname".
- Repeat your search on other search engines, like **DuckDuckGo** and **Bing**.
- Look for your name or nickname in the most common social networking platforms: are other people trying to impersonate you?
- Your name might be in the White Pages, together with your home address. The good news is that in some countries (like Mexico) there might not be a phone registry available online.
  - In Germany, you can check on DasTelefonbuch.
- In Germany, there are other search engines for persons. Try to find out if you get more results on them:
  - 11880.com
  - Das Örtliche
- If you have a website, check what information it reveals: go to a website that offers Whois domain lookup, for example Whois.com, and enter the domain of your website there: make sure that your personal details, like your home address, are not included there. If they are, you can request your domain name provider to anonymize this information. If they don't offer this service, consider moving your domain to a different provider. Access Now Digital Security Helpline is happy to provide help in identifying the most suitable providers for your needs. More info on domain privacy here.
- Many people have hobbies. Some are members of driver clubs, others are dog breeders, photographers, hikers, computer game fans, etc., and each of them have their own places for communication. When sharing on these platforms, some might believe that these exchanges have no relation to their jobs or other life domains, so they often publish more information about themselves there. Do you have a hobby? Visit your platform/s, check your profile/s, and review what you've published there.

Image searches

If you have a photo, icon, or avatar, you can do a reverse image search.

For example, if you use your portrait for your Facebook profile, you can check that this picture hasn't been used in other web pages by looking for the URL of your icon. To find out what the URL of your icon is, right-click the image and click "Copy Image Location", then paste the URL in a search engine.

A search engine will find all the pages that contain the image you are searching for. There are different search engines that can help you with this. Here we provide you with some brief information about some of them. For a more in-depth comparison of their features and further details about how to use them, please refer to the Bellingcat Guide To Using Reverse Image Search For Investigations.

- Google – Google is by far the most popular reverse image search engine – but its effectiveness depends on the search you are conducting. It may give you useful results for the most obviously stolen or popular images, but for more sophisticated research you might likely need to use more advanced search engines.
- Yandex – The Russian site Yandex is deemed as the most effective reverse image search engine currently available. In addition to looking for photographs that look similar to the one that has a face in it, Yandex will also look for other photographs of the same person – determined through matching facial similarities – which may have been taken with different lighting, background colors, and positions. While other – often more known – search engines like Google and Bing may just look for other photographs showing a person with similar clothes and general facial features, Yandex will search for those matches, and also other photographs of a facial match. If you need help with the Russian user interface, please refer to the Bellingcat Guide To Using Reverse Image Search For Investigations, which provides essential step-by-step instructions in English.
- Bing – Bing's "Visual Search" is very easy to use, and offers a few interesting features not found elsewhere. For example, it allows you to crop a photograph to focus on a specific element, and exclude from the search any other element which may not be relevant.
- TinEye – A fourth search engine that could also be used to do a reverse image search is TinEye, but this site specializes in intellectual property violations and specifically looks for exact duplicates of images.

Check if your online account has been previously compromised

Over the years, many company and platform databases have been breached, and the user names, email addresses, and passwords in those databases published online. You can find out if any of your accounts' credentials are included in these leaked databases by looking for your email on ';–have i been pwned?'.

If you find an account of yours was compromised, and you are using that same password for other accounts, you should immediately change that password. This could also be a good moment to set new strong and unique passwords and multi-factor authentication for all your accounts. The Access Now Digital Security Helpline team is happy to guide you in this process.

How to delete your traces

If you find sensitive information that you need to delete, in the European Union you can often rely on the right to be forgotten.

Access Now Digital Security Helpline is ready to guide you through the necessary steps.

- **Google**
  - To be removed from Google **searches** you can use this form
  - Request the removal of content on various Google **services** here
- **Facebook**: Request removal of photo or video because it violates your rights here
- **Instagram**:
  - Controlling Your Visibility
  - What should to do if someone shares an intimate photo without permission?
- **Twitter**: Report doxing or posting of private information here
- **Snapchat**: Help Center - Click on "Report a Safety Concern".
- **Reddit**: What to do if someone posted your personal information
- **Tumblr**: How to report a privacy violation
  - If the public form cannot help, abuse can be reported by email following these instructions
  - Email address: abuse@tumblr.com
- **Das Telefonbuch**: If you want to delete your entry, follow these instructions.
- If the personal information is on a website, you will need to contact the administrators and/or the host provider. Access Now Digital Security Helpline can help you identify the contact point.
- If someone is impersonating you on a social networking platform, Access Now Digital Security Helpline is ready to guide you through the necessary steps to report and take down that profile.

Further reading

- Online Harassment Field Manual, which includes the article Protecting from Doxing - PEN America. Last modified on December 17, 2020.
- Exploring Your Visible Data Traces – Me & My Shadow. Last modified on October 12, 2016.
- How to manage your online identities in a secure way, also including a section on self-doxing – Gender and Tech Resources, Tactical Technology Collective. Last modified on April 19, 2018.
- Self-Dox – Gender and Tech Resources, Tactical Technology Collective. Last modified on September 24, 2015.
- How to Survive the Internet: Strategies for Staying Safer Online – Yael Grauer. Published on November 21, 2014.
- Extreme Privacy. What It Takes to Disappear: Second Edition. Personal Data Removal Workbook & Credit Freeze Guide - Michael Bazzell. Last modified on June 2020.
- Self-Dox – School of Privacy.
- So What the Hell Is Doxxing? – Decca Muldowney, ProPublica. Published on November 4, 2017.
- Preventing Doxing – Crash Override Network. Published on January 17, 2015
- So You've Been Doxed: A Guide to Best Practices – Crash Override Network. Published on March 21, 2015.
- What to Do if You're Being Doxed – Lily Hay Newman, Wired. interviews Eva Galperin, Director of Cybersecurity at the Electronic Frontier Foundation. Published on September 12, 2017.

Resources for journalists and newsrooms:

- How To Deter Doxing. Newsroom strategies to prevent the harassment that follows the public posting of home addresses, phone numbers and journalists' other personal information – Rose Eveleth, Nieman Reports. Published on July 17, 2015.
- How to Dox Yourself on the Internet – Kristen Kozinski and Neena Kapur, The New York Times. Published on February 27, 2020. The article also recommends additional resources by the New York Times Digital Security Education Hub, including A Guide to Doxxing Yourself on the Internet, Social Media Security & Privacy Checklists and a Doxxing Curriculum Guide to help trainers with designing workshops for journalists and newsrooms.

Tags: