#NotOk

How to Doxx Yourself?

Doxxing is a practice where individuals with malicious intentions and troll, track down personal information about a person, such as their home address, phone number, place of work, their children's school, and other personal details that they can find. Unfortunately, many of these details can be accessed through public databases or social media, and perpetrators often use this information to intimidate or threaten their targets.

Journalists are particularly at risk of being doxxed, but there are measures you can take to protect yourself. Self-Doxxing will allow you to make informed decisions about what information is shared online and what you want to share .

Discovering personal information available online can always be unsettling. However, this guide will help you minimize the risk of your private information being used against you.

In order, to properly protect yourself you need to think like a doxxer. Ask yourself the following questions :

- What are we looking for?
- Where could we find such personal information? What are the platforms we might want to use to find them?
- How can this information be useful? Where might it lead us ?

Once you have determined the information you are seeking, the guide can assist you in checking if it is available online

Step 1 : Check yourself on Google

First do a search on Google: Start by searching for your name on Google and other search engines. This will give you an idea of what information is available about you.

1. Type your name into the search box. Review the search results: Scroll through the search results to see what information is available about you online. Take the time to examine the different sources where you appear.
2. Refine your search: by adding additional search terms, such as your location, profession, or education you will get more precise results.
3. Reverse image search : you can conduct a Google Image search to find out where else your photographs are being used and how. You can add your profile pictures from LinkedIn, Twitter, Facebook, and Instagram.
4. Do the same research on different search engines such as : Bing, Yahoo, DuckDuckGO.

Pro tips:

- You can use the following search operators for Google and Bing to refine your results :

Google & Bing Search Operators		
Operator	**What it searches**	**Example**
Site	Provides results of pages located on a specific domain	site: linkedin.com
AND/OR	Use the AND operator to return results containing two results. Use the OR operator to return results that contain one result or the other result.	“John Doe” AND (Toronto OR Montreal)
Asterisk	Google treats the asterisk as a placeholder for a word or words	“John * Doe”

	in a search string.	
Hyphen	This operator allows you to exclude the text immediately following it.	“John Doe” -site:yournewssite.com
Filetype	Filter search results by a single file type extension Common File Types: ● DOC/DOCX ● XLS/XLXS ● PPT/PPTX ● TXT ● JPG/JPEG/PNG (Image files) ● PDF	filetype:xls intext: you@youremail.com

<u>Recommendations </u>:

- Consider when and where you give out personal information online. For example, if you sign an online petition, there is a risk that your information will be potentially published.
- You can also set up Google Alerts for your name to receive notifications when new information about you is posted online. Once you’re signed into your Google account, you can set up Google Alerts here: https://www.google.com/alerts.
- Start by reviewing your bios, CVs, and personal websites to identify any personal information that is publicly available. Use advanced search techniques such as search operators to locate any PDFs of resumes or CVs that may be publicly available. For any resumes or CVs you discover, remove your home address, private email, and private cell number and replace them with your professional contact information.
- Limit location-tracking on your phone. Check the settings for each app on your phone.

It's always useful to Google yourself regularly to stay aware of what information is available about you online.

Step 2 : Audit your Social Media

Some settings are often set as 'public' by default, which encourages you to disclose certain personal information without realizing that others may have access to it. Attackers will look for personal information to use against you through your social media accounts.

Be strategic about which platforms you use and for what purposes. If you're using a platform for personal reasons, like sharing pictures with friends and family on Facebook or Instagram, tighten your privacy settings. However, if you're using a platform for professional purposes, such as tracking breaking news on Twitter and tweeting links to your work, you may decide to leave some settings public. In that case, avoid posting sensitive information and images, such as your birthday, phone number, location, home address, and family members'/friends names and photos.

1. Make a list of all your social media accounts: Write down the names of all the social media platforms you use. Determine what is the use of each account: is it used for professional purposes ? personal ? both?
2. Review your posts: Go back through your old posts and make sure that you are comfortable with the information that you have shared in the past. If there is anything that you don't want to be publicly available, consider deleting it or archiving it.
3. Review your privacy settings: Go through the privacy settings on each platform to ensure that you are comfortable with the information that is being shared with others. Adjust your settings as necessary to limit who can see your profile and your posts.
4. Remove any inactive accounts: Use databases like Peekyou or Namecheckr to see where your common handle is being used. If you have any social media accounts that you no longer use, consider deleting them or deactivating them .
5. Review your location settings. Disable location settings on your various platforms to ensure that your social media posts, photos and status updates do not share your location in real time.

Pro Tips :

- Use the “**View as**” option on Facebook to see how any Facebook account can view your profile.
- Use a private browser to find your other social media platforms and see what information is publicly available.

Recommendations

- Take the time to go through the different security settings of your social media platforms and configure them as you see fit.
- Before posting content on social media, take time to review it and try to determine whether it contains information such as your location, contact details or information about your loved ones. Look at the different angles of your photos. Could there be a clue about the area you live in (e.g., is your street identifiable by a distinctive sign, a wood, a school, a store)?
- If you consider using different social media profiles for professional and personal purposes, consider using a pseudonym on your personal account to make it harder for trolls to find you.
- Regularly auditing your social media accounts can help you maintain control over the information that is available about you online.
- It's important to remember that family and friends may also be at risk of doxxing. If you believe you’re at risk, have a conversation with your loved ones about their internet usage and what information they reveal about themselves and you online.
- Use the block, mute or restrict options on your various social media platforms if you receive unsolicited abusive content.
- Follow our top recommendations for Social Media below :

- Make sure personal photos are only accessible to a certain group of friends
- Hide your friend list from public view
- Do not share information in real time
- Edit who can look up your profile using your email or phone number
- Disallow search engines from linking to your profile
- Review how others can interact and post to your timeline
- Review who can tag your account in posts and pictures
- Block comments on certain photos
- Avoid identifying family members and friends
- Delete or archive any photos that might reveal personal information (e.g., where you live)

- Option to have a private or public account
- If you want to keep your account public, make sure that some users are not able to tag you or mention you in photos, videos and comments
- Delete or archive any photos that might reveal personal information
- Share your personal stories only with your close friends (make sure this list is up to date)
- Avoid identifying family members and friends in your personal photos
- Instagram also offers the option to disable comments under your posts

---

- Information can be distributed VERY quickly on Twitter, which is why it's important to take your time before posting certain photos or personal information on that particular platform
- Apply quality filters
- If you don't feel comfortable receiving messages from an unknown user, disable the Allow message requests from everyone setting
- Disable photo and location identification
- Use the mute words and hashtag option. Twitter will automatically remove all tweets containing these words or hashtags from your News Feed
- Edit who can look up your profile using your email or phone number
- Go over your old tweets

Step 3 : Review online directories

Address search

Check online directories like Canada411 to see if your name, address or phone number appears. Without knowing, your home address or your phone number might be available on this database. To remove that information you will need to send a request through the platform. See recommendations below.

Pro Tips:

- When conducting this type of search, be specific about the area you live in. Results may not appear if you search for a larger zone (e.g. you live in Vaughan, but you enter Toronto in the search bar).
- Search for your relatives on this database. Their names might have been displayed on your photos or comments and possibly their information is available on those databases.

Recommendation:

- If the information is on Canada411, the removal process is quick and easy. You will need to make a request by clicking on the link below (it takes two working days for the information to be removed). You will also need to ask your telephone operator to change your telephone number to a private number (this request may take longer) : https://www.canada411.ca/help.html?key=faq.

Step 4 : Monitor data breaches

Your personal information may be compromised in a data breach. Haveibeenpwned.com allows you to determine whether any of your email accounts were affected by a significant data breach.

Recommendation:

- Change the password for any affected accounts right away, and don't use it again. You may also use a password manager if you fear that you may forget your password. A proper password manager is usually equipped with dark web and data breach monitoring; some even send proactive alerts to warn you that your data has been compromised.

Public records

In Canada, public records are generally held at the provincial or federal level, and the types of records available to the public may vary depending on the jurisdiction. It is important to note that not all public records are freely available to the public.

Some may require authorization or payment to view, and others may contain sensitive or confidential information protected by privacy laws. Unfortunately, we cannot request the removal of public information that is available to all citizens.

However, it is important to take into consideration that these databases exist and to keep this in mind to safeguard certain personal information online so that you do not provide perpetrators with additional details about you.

1. **Vital records**: These are the official records of births, deaths and marriages that are usually kept by the provincial or territorial government. Although marriages and births are not publicly available, deaths can be easily found on the internet and usually include the names of your relatives. Someone with malicious motives can find you through the social media platforms of your relatives.
2. **Property records**: These records include information on land ownership, property values, and property boundaries, and are typically maintained by the provincial or territorial government.

3. **Court records**: These records include information on legal cases, judgments, and decisions, and are typically maintained by the courts and can be accessible to the public. Depending on the record (criminal, civil or municipal) an address and date of birth may be disclosed.

4. **Corporate records**: These records include information on businesses registered in Canada, such as their names, addresses, and business activities, and are typically maintained by the federal or provincial government.

5. **Electoral records**: These records include information on voter registration and electoral results, and are typically maintained by the federal or provincial government. Depending on the province, you are able to see if an individual is registered on the list of electors. This makes it easy for a perpetrator to check whether you still live at a certain address or not.

6. **Other government records**: Some records contain valuable personal information on movable property and persons. The different provincial governments manage these databases.

Other Information Security Recommendations

- Keep your professional and personal email and as well as phone number separate. Use your professional accounts only for work related purposes. Be cautious about how much identifying information you include in your email signature.
- Use two-factor authentication: Two-factor authentication adds an extra layer of security to your social media accounts, making it more difficult for hackers to gain access.
- Be careful with third-party apps: Be cautious when granting access to third-party apps that request access to your social media accounts. These apps can sometimes be used to collect your personal information.
- Use a secure messaging system if you need to discuss with a source or need to share personal information.
- Consider using a VPN: A virtual private network (VPN) can help protect your online privacy by encrypting your internet connection and masking your IP address.
- Be aware of phishing scams: Be cautious of any suspicious links or messages you receive on social media. These could be phishing scams that attempt to steal your personal information or login credentials.
- Check your app permissions regularly and revoke access to any apps that you no longer use or trust.

By taking proactive measures to protect your personal information online, it will help reduce the risk of being doxxed. Remember to limit your online footprint, secure your social media accounts, be careful where you share your personal information, use secure communication channels, take the time to doxxed yourself once in a while, and have a conversation with your friends and family about the risks of doxxing.