onlineharassmentfieldmanual.pen.org /protecting-information-from-doxing/

Manage Your Online Footprint

15-19 minutes ⋮ 4/9/2018

Online harassers who wish to intimidate and silence you can weaponize your personal or sensitive information to make you vulnerable to additional attacks.

Source: cybervisuals.com, Illustrator: Bronny Hui

We live so much of our lives online, and so much information about our personal lives is just a Google search and a click away from an abuser's fingertips. Abusive trolls, cyber mobs, and other bad actors take advantage of our public online footprints for a variety of malicious ends. Sometimes they might use this information to try to impersonate you online to tarnish your reputation. Or they might use this information to target you with personalized, identity-linked attacks.

Another common and dangerous tactic online abusers use is to "dox" their targets by posting in a public forum a target's personal information like their home address, personal phone number, the name of their child's school, or any other personal information they're able to find. (You can learn more about different types of online abuse here.)

Writers and journalists who write about controversial topics are particularly vulnerable to doxing and impersonation. Whatever the particular tactic a harasser tries to use to target you, there are some steps you can take to protect yourself by controlling your privacy and managing your online footprint.

STEP 1: Start by Googling Yourself.

Google variations of your name, your phone number, your past and current home addresses, your email addresses, your close family members, and your usernames and handles. Make sure you're not logged into Google (which could skew your results). You can also try different search engines, like Bing and Yahoo. Take advantage of these Google search tips.

Look at the image results too. Right-click on each image and then select "search Google for image" to see where else your photos are circulating and how they're being used. You can also upload your profile photos from your social media accounts to Google image search, and try a reverse image search using a platform like Yandex or TinEye. Just don't upload images that are sensitive or private!

- What kind of info are you seeing floating around? And where is it cropping up? Social media accounts, staff bios, company websites?

How You Can Take Back Control

So you've discovered what's out there and you might be feeling unsettled. Now what? The good news is there are steps you can take to remove existing private information and reduce the chances of it cropping back up. While there's no silver bullet to safeguarding your privacy and your safety online, the goal is to make it harder for an abusive troll to cause you harm.

- **Delist your personal information from Google**
  You're able to request Google to remove your personal information from their search. Here's a step-by-step guide, by Yahoo's technology editor, that details the process. It's important to note that you should select the option to remove your information from both Google search and other sites.
- **Set up Google alerts**
  For your full name, your phone number, your home address, or other private data you're concerned about so you know if it suddenly pops up online, which may mean you've been doxed.
- **Contact website publishers**
  Maybe you found an article about you from 10 years ago on your high

school newspaper's website or on your mom's blog. Wherever the information is published, if you're worried that it can be used by a bad actor to harass you, contact the website's owner or publisher and ask them to remove it.

- **Review your own website and bios**
  If you have a professional website for your work or a blog, review it to make sure you're not providing your personal contact information or other data about your personal life. To see if you've got PDFs of résumés or CVs floating around the web, try Googling the following: "[First Name] [Last Name]" filetype:pdf. (Those kinds of advanced searches are called "Google dorking" and, while dorky indeed, they're very useful.) For any résumés or CVs you discover, be sure to get rid of your home address, private email, and private cell number (or replace them with public-facing versions of that info).
- **Ask your workplace, university, or volunteer affiliations not to publish your contact info in their online directories**
  See this Field Manual's Guidelines for Talking to Employers and Professional Contacts if you'd like tips for discussing online harassment in a professional capacity.

STEP 2: See What Data Brokers Have on You

In the U.S., people search engines–like Spokeo, Intelius, BeenVerified, and Nexis, etc.–scan the web to collect your private information and then sell it to companies and individuals, or to other data brokers. This problem is particularly acute in the U.S. because of lax privacy regulations, but it is not exclusive to the U.S. Wherever you work in the world, it's important to research what information people search sites have on you.

How You Can Take Back Control

While it's nearly impossible to prevent data broker sites from collecting your personal info in the first place, at least you can get a lot of it taken down.

- **Opt Out Manually**

While it's labor-intensive, you can have your information removed for free. If you are based in the U.S., start with the three major wholesalers: Epsilon, Oracle, and Acxiom. Check out the Big Ass Data Broker Opt-Out List and Optery's Opt-Out Guides for directions on how to remove your information from each of these and dozens of other data broker sites. After you've removed your information from the big three wholesalers, proceed with whichever sites top search results when you Google yourself. You'll have to get into the habit of checking these databases twice a year, because your information can be republished even after it has been removed. For more in depth guidance on how to get your data scrubbed from data broker sites, check out this helpful article from Consumer Reports.

- **Purchase a Data Removal Subscription Service**

There are services that remove your information from data broker sites for you in the United States. These include:

- **DeleteMe** ($103/year, see their pricing plans here & use discount code PEN20)
- **Kanary** ($144/year, see their pricing plans here)
- **Optery** (offers a range of plans, from a free self-service plan to tiered pricing)

Note, these services rely on human beings to request the removals for you. Your data will not be scrubbed instantly. Also note that these services may not remove your information from every data broker site, but they do save you a lot of time.

STEP 3: Audit Your Social Media

Trolls comb through social media accounts looking for private information they can leverage against you—an embarrassing tweet you forgot about, a photograph that gives away location information. Abusers also look through your social media to find doxable information, like where you live or who your close friends and family members are.

How You Can Take Back Control

There are few black and white rules for privacy settings on social media, but we'll provide you recommendations for how to optimize for privacy and limit harassment. You can choose which ones are right for you at this time and toggle them on and off as your circumstances and needs change.

- **Keep your private life private and your public life public**

Be strategic about which account you use for which purposes. If you're using a social media account for personal reasons (like sharing photos of your vacations or your pets on Instagram), make your account private and tighten your privacy settings. Don't reuse that account to contact sources, clients, or connect with your audience. Make a second account on that platform if you want to use it for professional purposes. If you're using an account for professional purposes (such as tracking breaking news on Twitter and tweeting links to your work), you may decide to leave some of the settings public—in which case, avoid including sensitive personal info and images (your birthday, phone number number, location, home address, family member’s names and photos, etc.).

- **Tighten your settings on social media.**
  Below are links to the privacy settings for several major platforms.
  - Google
  - Facebook
  - Twitter
  - Instagram
  - TikTok
  - LinkedIn

For a deeper dive, check out PEN America’s Digital Safety Checklist and the New York Times’ Social Media Security and Privacy Checklists.

- **Monitor data breaches.**
  When there’s a catastrophic data breach, your private info can be compromised. You can check to see if any of your email accounts were part of a major data breach via Haveibeenpwned.com or Firefox Monitor. For any affected account, change the password ASAP and don’t use it again. You can also set up an alert on the aforementioned site to find out if any of your accounts are part of data breaches in the future—just use the site’s “Notify me” tab.
- **Audit your social media.**
  Abusers comb through social media accounts looking for private information they can leverage against you—an embarrassing tweet you forgot about, a photograph that gives away location information. Social media platforms also want you to share as much of your personal information as possible, so they often bury the privacy settings on your accounts and default those settings to “public.” Data brokers benefit from lax privacy settings, which make it easier to scoop up your info.
- **Review your bios, CVs, and personal websites.**
- **Establish separate email accounts for separate purposes.**
  You want to have at least three email accounts: professional, personal, and “spammy.” Your personal email address is for private correspondence with close friends, family, and other trusted contacts—best not to list this address publicly. Your “spammy” email is used to sign up for accounts, services, and promotions. The email you use for work (whether you’re a freelancer or affiliated with a particular organization) is what you can list publicly. As with public-facing social media accounts, you may want to be sparing in how much identifying information you include in your email handle (eg, full name, ethnicity, birthday, religion, location, etc). Browser extensions, such as Firefox Relay, allow you to create and share email aliases instead of your real email address to protect both your inbox and your identity.

- **Tighten your settings on social media.**
  Be strategic about which platforms you use for which purposes. If you're using a platform for personal reasons (like sharing photos with friends and family on Facebook or Instagram), tighten your privacy settings. 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 of the settings public—in which case, avoid including sensitive personal info and images (your birthday, cell number, location, home address, family member's names and photos, etc.). Below are links to the privacy settings for several major platforms. For a deeper dive, check out PEN America's Digital Safety Checklist and the New York Times' Social Media Security and Privacy Checklists.
  • Google
  • Facebook
  • Twitter
  • Instagram
  • TikTok
  • LinkedIn
- **Review your location settings.**
  Check the location sharing setting. on each app on your phone. Start by restricting location-tracking on as many apps as possible; otherwise, your location data can be sold by shady apps to even shadier data brokers. To ensure that your posts, photos, and status updates on social media are not sharing your location in real time, check the settings for each platform and turn off location services.
- **Remove Hidden Exif Data From Photos**
  You might also consider scrubbing the metadata on all photos you post online. Photographs today contain much more than the image itself—they have information and lots of it. Every time you take a picture on a digital camera, an Exif file is created, which contains all kinds of data on that image, including the date, time, and location at which the photo was taken. When you share your photos, you could inadvertently share potentially sensitive information that could put you and others at risk. While some social media platforms remove the Exif data from your image-based posts before they're shown to others, other sites, like Flickr, have a default setting that leaves Exif data publicly available. To scrub metadata from photos, you can use a tool like ImageOptim or you can use this PRO TIP: download the Signal messaging app, text photos to yourself (which automatically scrubs their metadata), and then save the photos back to your phone. To learn more about how to remove Exif data from your photos, see Consumer Reports' How a Photo's Hidden 'Exif' Data Exposes Your Personal Information.
- **Be conscious about third-party apps and services.**
  When you're prompted to create a username and password for a new software or service, have you ever selected the option to "sign in"

automatically via Google or Facebook? If so, you may have given this third-party software or platform a back door to track your account and to try to access permission to view your contacts, photos, location, etc. It’s best to avoid creating accounts directly via Google or Facebook; instead, you should use a password manager. Android users can also use a privacy auditing platform, like Exodus Privacy, which looks for and lists embedded trackers to help users improve the privacy of their smartphones.

- **Be your own personal content editor.** Consider when and where you give out personal information online. Keep in mind that when you sign an online petition, the website owner could potentially choose to publish your information. Review all text in your tweets, Facebook messages, Instagram posts, etc. before you publish. Is there any personally identifying information about your location? Your contact information? Your loved ones? If you feel vulnerable to an online attack, it’s worth editing the text. Pro Tips: 1) To see what’s publicly available, be sure to log out of your account; 2) to see what’s visible to friends, ask a friend to pull up your account and screenshot it.
- **Consider using a pseudonym.** For many writers and journalists, this may not be an option—your name may well be your bread and butter, or you may take pride in associating your name with your published writing (as you should!). But if you have the flexibility or desire to use a pseudonym when publishing an article you know could be subjected to hateful online backlash—especially if you’re a writer just starting out in your career or undertaking a project unrelated to your everyday professional life—a nom de plume can save you from being targeted by more severe forms of online harassment while still ensuring that the public has access to your writing. This Gender and Tech Resources Manual, a project of the Tactical Technology Collective, offers additional guidance on this subject.
- **Remember: Your family and friends may be at risk of doxing as well.** If you believe you’re at risk for becoming a target of doxing, it can help to have a conversation with loved ones about their internet usage and what information they reveal about themselves online. You may also want to respectfully ask them to be careful about what they post about you and whether they tag you. High-profile targets of doxing can end up inadvertently exposing family members, especially if they’re a writer who covers a particularly controversial beat.

If you need help implementing any of the guidance above or want to delve a little deeper, check out these fantastic, interactive, and user-friendly toolkits: Security Planner from Consumer Reports and Cybersecurity Toolkit for Journalists from the Global Cyber Alliance.

The guidance above is adapted from the article Why You Should Dox Yourself (Sort Of), published on Slate.com in February 2020 and was developed in consultation with cybersecurity experts at Freedom of the Press Foundation.