HOW TO DISAPPEAR ONLINE

Disappearing online can be difficult, but it's not impossible in most cases. This security guide will discuss methods that you can use to avoid being found online by a stalker or abusive ex-partner, while retaining your freedom to communicate with people of your choosing. The goal, then, isn't to remove your presence entirely but to control it wherever possible.

Find yourself first

The first step is to figure out how large of a "digital footprint" you already have. What information about you is already available and where can it be found? Open up your browser in incognito / private browsing mode and make sure you're not logged into any services like google or social media sites, then start searching for yourself. In addition to whatever else you think may apply to you, search for the following specific items and document your findings:

- Your full name
- Any unique nicknames
- Email addresses
- Usernames
- Phone number

After that initial search, start combining them for even more granularity. Also add other pieces of information like your past city, current city, and so on. Be creative and thorough, and use as many resources as possible in order to build a complete profile.

Next, make a second list of all the accounts that *you* know you have but that you didn't find in your search. These still represent a risk and need to be considered.

Reduce your footprint

Go through the list you just created. Think about which of those accounts you want to keep and which ones you don't need any more. Unless you're keeping a dormant account open to provide a decoy (which we'll cover later in this guide), you should close it. Some sites will allow you to remove your information prior to closing your account, so make sure to research that or contact the site prior to closing your account to find out how to do that.

For any "people search" results that you find, look for options to opt out or have your results removed from the search. Take a look at our other guides for more information on this. Make sure to look for cached versions of

the results on the Internet Archive (archive.org); if you find any results there, contact them and provide a link to your information and they will remove it.

Decoy accounts

It's not always possible to remove yourself completely from internet searches and social media. Once you've reduced your footprint as much as possible, the next priority is to introduce misleading and decoy information to make it harder to someone to find anything real about you. Because they would have to spend time and energy looking through inaccurate information and false leads, they're less likely to find your actual accounts and may disregard them if they do. Setting up decoy accounts is one way to introduce "noise" into the search results.

Your decoy accounts should be relatively easy to find and active. They should also look very convincing in order to be effective. To do this, you can either continue to use existing accounts but add misleading information, or you can create new accounts just for this purpose. Whichever you choose, under no circumstances should your real and decoy accounts be connected in any way. For example, don't use the same email account for your real and decoy accounts and don't friend, follow, or connect them together.

You should develop at least one convincing persona, but remember that your safety increases as the amount of misleading information about you goes up. So consider ways that you can subtly plant information in different ways that may ultimately be found by someone that you don't want to find the actual *you.* When developing a persona (which in all regards would appear to be you), take time to make it convincing. Where do "you" live? What college do you attend and what classes are offered there? Your decoy persona should be difficult to discern from your real one. Some ways to do that include:

- Mention a regional restaurant chain at dinnertime in that time zone
- Follow local businesses, politicians, or sports teams
- Complain about the local weather (you can use a weather app or website to find out what you should complain about)
- Reserve a Google Voice number using the area code you're claiming as your own
- Discuss local happenings or news events
- Remember the time zone that your persona is in and post accordingly. You can use a free tool like Hootsuite to schedule tweets for certain times

Remember that details are what makes a convincing profile. Don't make every post an overt hint about your location, or it might appear *too* obvious to be real. Make comments that you would normally make, just be

careful not to give away too much. Consider also getting trusted friends or fake accounts to interact with your decoy profile to further increase the seeming legitimacy of the information.

Consider also creating multiple accounts using your name but without any other identifying information. For example, an Instagram account with only funny cat pictures. This would create even more static while also drowning out any "dox drops" (that is, personal information that might be posted about you). And don't forget about an Amazon wish list! If you haven't disabled it, consider seeding it with planned purchases that would support the decoy account. For example, you might live in Arizona, but your decoy lives in Virginia. Which one would be more likely to buy heavy clothing and boots in the winter?

The end state is that your real accounts will be difficult to find and your decoy accounts will be easy to find.

Social Media

You may wish to keep or create one or more social media accounts in order to communicate with your friends, loved ones, and your support system. There's nothing wrong with using social media, but it's important to be smart about how you do it. Make sure to review the social media security guide on this site, but here's a few things to keep in mind:

- Take advantage of privacy settings. Limit your account's visibility to only those you trust and don't allow your profile to show up in search results.
- Use account security features, like two-factor authentication and strong passwords
- Consider using a fake name or a nickname if possible and allowed under the terms of use for the service. Only trusted individuals should know the name that you use for those accounts
- Even on your "real" account (that is, the one you actually use to communicate with your trusted contacts), use fake information wherever possible. Consider using a random date as your birthday, a false address, etc

Create a "Tripwire"

A tripwire is a method you can use to see if anyone's following the fake leads you planted to protect your true identity. While it may generate false positives, it can be an indication that someone is trying to find your actual location and give you time to react or increase your privacy posture. While there's many ways you can accomplish it, the key is to set up a trigger that would alert you if a certain action is taken.

For example, your decoy persona naturally has a job. You can create that fictional business from scratch and make it appear legitimate; that means you control the website, email address, and phone number (through

Google Voice or some similar service). Monitor the "business" mailboxes; anyone asking about you specifically or asking even asking general questions might be an indication that someone is trying to find you.

Search Engine Optimization

Search Engine Optimization, or SEO, is the process of causing a website or page to show more prominently in search engine results. This is often used by businesses to make themselves easier to find, but the process can also be used to make yourself harder to find online. You can create multiple pages using free online tools that will rise to the top of search engine results and make your actual information, to include information over which you have no control, harder to find.

Unlike businesses that have to optimize their site for a wide variety of search patterns, you know exactly what search terms you're targeting. Because those are very specific and likely exact terms, it's relatively easy to get your desired pages higher up in the results. Even though your pages aren't likely to have much "page rank" (a general term for the "importance" of a webpage from a search perspective), the specificity of the terms will compensate for this.

There are many free website builders available online. Just searching for the term will come up with many great options. Some of those include wix.com, webs.com, and wordpress.com. You can use any of them or all of them. WordPress is a good option to start with, because it's easy to use and has SEO options built in. Create a page using information that the abuser is likely to search for, such as your name, username(s), or other pieces of common information that's worked into the profiles or bios.

Once you have the key information on the page, you can add other information either as a decoy or just to add more noise into the search results. Once again, the goal is to make your actual information hard to find by someone that you haven't specifically shared it with.

Don't Commit Crimes

This is probably a good idea for many reasons, but don't do anything that would be recorded in public arrest or trial records. Even speeding tickets can often be found by searching county court databases, which can give information about your location.

Other Tips

- Avoid using your real name for real information whenever possible
- Don't use the same usernames for your real accounts as your decoy accounts
- Always use strong passwords and two-factor authentication
- Verify new friend requests before accepting them
- Remove metadata before sharing images or documents
- Use fake information for account security questions. Make sure your abusive ex-partner can't guess your answers
- Change all passwords for accounts that your abuser had access to
- Educate your children and trusted friends about what they can and shouldn't share online
- If using a shared computer, always log out
- Don't click unfamiliar links or open untrusted attachments
- Don't click on shortened links unless you're 100% of the source
- If using your own computer but others have access to it, always log out of your accounts
- Just don't use a shared computer if you can help it
- Use the other security guides on GoAskRose.com
- Think about everything you post online. Can it be used to find you?
- Use a VPN to avoid being tracked by your IP address

Although it can be a lot of work, you can make yourself very difficult to find online. By following these steps, you can limit your exposure while drowning out the accurate results that you need to hide. The end state is that you can control who you communicate with and keep yourself safer on the internet