# How not to get too doxxed

Just bolting together some specific advice about how to keep your online identity away from your personal life. It's not a comprehensive guide, and is really just aimed at limiting the damage. It is very unlikely that you will be able to clean up every breadcrumb, and you only have to fail in defence *once* for information to be irrevokably leaked online.

# Do your own research

If you can find your own stuff by searching for your real name, you're likely pretty doxxable. Especially if your online name links to a domain or email address that has been registered with your real name. That includes stuff like payment accounts, archive.org history, Facebook accounts after the real name policy, etc.. Do that search, and get comfortable with anything there being used against you online. If it links to people close to you, it may be worth thinking about when and how you'll give them a heads up (i.e. let your work know if you show up on an *farms site). Clean up anything you can, shut down unused sites, delete unused accounts. They may not be gone, but they will be harder to find.

# Don't let people join the dots

The most common way your details will get out there is if you have a link to a government or institutional account. Banking, drivers licenses, ID confirmation, KYC stuff, is all pretty obvious, but consider who you give things like phone numbers, email addresses, and other ID-type things to. These can be quickly used for confirmation (i.e. if I think I know your phone #, and have your twitter ID, I can use the recovery form to confirm some digits. You can do this with credit cards too if you can get a glimpse of an account, or if you can hack another online account that shows payment history).

Be mindful of things that will let people link up IDs. IP addresses can also be here (will touch on them later). Details like phone numbers, email addresses, portions of credit cards, etc. can be used to confirm a dox. If you can, use things that are only for your online identity

# Do the basics

Basic online hygiene. Get your PC up-to-date (i.e. make sure Windows Update is running and current), make sure you have anti-virus (Windows Defender is good, built in, easy to use). That's baseline. Add to that: Do not click any links you are sent unless you know what it is and know the site, this is how people get IPs for DDoSing, confirming, etc.. If I see an IP from a rough area I know someone is from, I can probably get within 30km of that person's address, but I can also do things like port scans to see if you are running any home services, or present any other vulnerabilities.

# Compartmentalise

Separation, separation, separation. As much as possible, don't let your online and offline lives blend. Separate email addresses, separate names, etc. - but if you can also separate discord accounts, separate social accounts, separate twitch accounts. Thinks like Steam URLs that haven't been updated in years, old tweets with your new car (and new car rego), etc. - those are pretty obvious. But add in - your friends socials where they are linked to you - consider just blocking anyone on your online accounts that you know in real life that uses their real details online (especially if they may post your face and real first name).

# Don't feed these sites

Do not interact with sites known for doxxing. Especially if you haven't cleaned up your online. These account records are available to site owners, and things like search terms you enter, Google referrers (i.e. what you used to search for them), places you link to the site, your IP, any browser fingerprinting, etc. becomes immediately available to them. If you absolutely have to interact, use something like the Tor Browser and make sure you visit in a totally clean session. Never enter any information directly into these sites.

# Keep yourself clean

Keep things 'clean' - don't stay in too many discord servers (know that your server join list is public), don't keep accounts open you don't need, don't get lazy and use an existing personal account for something. These are the places that your ID will leak. Some things (like WHOIS records, anything on Wikipedia, anything that's a public record) are there forever so it only takes one slip-up.

# Watch yourself

Make sure you have good visibility - sign up for Google Alerts for your real name on your personal Google Account, sign up for https://haveibeenpwned.com/. Repeat your initial search on a semi-regular basis. Ask people to check up on you from time-to-time.

# Max Security

Like with the online hygiene - max out your security settings. Set up MFA everywhere, but do not use SMS verification if you can turn that off. Phone numbers can be stolen very easily, and SMS is not a secure medium. Use a password manager and do not reuse passwords. **If your password leaks it can be used to tie two unrelated accounts together.**

# Don't Freak Out

Do not freak out - if your info shows up online or on stream, just don't interact with it, move it off screen if you can while streaming. It is very important you don't provide confirmation, or an indication of something to be clipped. If some info leaks - do a set of Google searches for all the info, to get a sense of how far it goes. For things like IP addresses, this won't be very far - but consider how that may come back to you. An IP address can be used to DDoS you, a PO box can be used to send you awful things, and a home address can swat you.

# Plan to Fail

If someone is really after you, there is probably very little to do to stop the dox getting out. Have a plan for when that happens. Know what you're scared of (Job? Family? Etc.) and have a plan to inform them - i.e. you can say to HR at work 'some Internet weirdos may try get me fired by lying about me, because I helped out with a politics server online', you can say to your family 'you may get some harassment - don't engage with it, report it to the cops'. If you think there's a risk of swatting - let the cops know on their non-emergency line, it won't stop it happening, but it will let you establish a pattern (i.e. not 'just a prank') of harassment that can help law enforcement get involved.

If anything happens in the real world - ***tell the police***, it is a federal crime almost everywhere, and will massively help if things spiral. (i.e. "No, Mr. Boss, I am not a <horrible thing>. Here's a copy of my police report about how I'm being harassed" will help you clearly define who the victim is).

---

Revision #4
Created 17 October 2022 00:09:36 by Bossett
Updated 17 October 2022 00:32:42 by Bossett