How to prevent doxxing - DeleteMe.pdf
Saved to Dropbox • Apr 9, 2021 at 12:06

DeleteMe

How to prevent doxxing?

Laura M
September 11, 2020

Unwittingly escalating an online argument is regrettably easy. One minute, you're replying to an internet troll's comment on Youtube. The next, you've been doxxed. If you're lucky, you might get away with a few annoying messages or several hundred dollars worth of pizza delivered to your house. But if you're unlucky, your life could become a living nightmare.

That's because whether you know it or not, your personal information is available to more or less anyone willing to look for it online. Although your Facebook profile is a treasure trove of information for malicious actors, your social media accounts are only partly to blame. Your home address, phone number, and email address are also out there, just waiting to be exploited by doxxers.

Keep on reading to learn more about doxxing, who is most likely to fall prey to it, and what you can do to protect yourself before and after a doxxing attack.

How Doxxing Happens

Photo by Sharon McCutcheon on Unsplash

Doxxing (or doxing) happens when someone discovers the real identity of an internet user and shares their personal information publicly. Most doxxers acquire personally identifiable information via people search sites, social media, and forums. Some might also hack their victims' devices or target them with phishing attacks.

According to the paper Fifteen Minutes of Unwanted Fame: Detecting and Characterizing Doxing, there are four general motivations for doxxing:

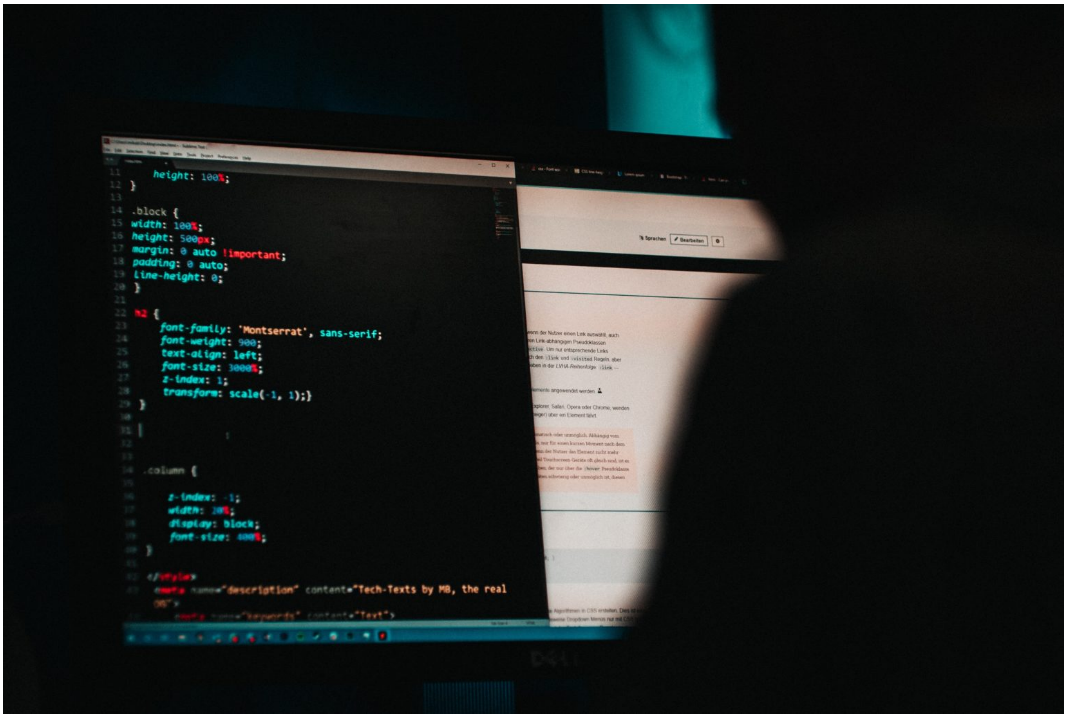
1. **Competitive.** The doxxer wants to show off their abilities or prove that the "undoxable" target was, indeed, doxxable.
2. **Revenge.** The doxxer wants to get back at their victim for something they did, like being an "attention whore" on a forum or beating them in an online game.
3. **Justice.** The doxxer attacks their victim because they did something immoral, like scammed someone on an online forum.
4. **Political.** Doxxing someone in support of a larger goal (for example, revealing the identities of KKK members).

Doxxing typically encourages other people (i.e., those who had nothing to do with exposing someone's information) to use leaked information for intimidation or harassment.

High-Risk Activities

The risk of doxxing can be elevated through certain activities. These include, but are not limited to, hacking, gaming, working in public-facing professions, reporting, and activism. However, it's worth remembering that anyone can fall victim to doxxing if they get on the wrong side of a bad actor.

Hacking



```
    height: 100%;
}

.block {
width: 100%;
height: 500px;
margin: 0 auto !important;
padding: 0 auto;
line-height: 0;
}

h2 {
    font-family: 'Montserrat', sans-serif;
    font-weight: 900;
    text-align: left;
    font-size: 3000%;
    z-index: 1;
    transform: scale(-1, 1);}
}


.column {

    z-index: -1;
    width: 20%;
    display: block;
    font-size: 400%;
}

</style>
<meta name="description" content="Tech-Texts by MB, the real
OG">
    <meta name="keywords" content="Text">
```

Photo by Mika Baumeister on Unsplash

Most doxxing targets are hackers, or people with accounts on websites, forums, and other internet communities related to hacking or cybercrime.

In fact, the term "doxxing" comes from the slang "dropping dox" ("dox" being "docs" or "documents"), a revenge tactic popular among hackers in the 90s. Back then, exposing their rival's identity and thus opening them up to harassment and legal repercussions was one of the few ways hackers could get revenge on their opponents.

What you can do to prevent doxxing: Conceal your IP address with a VPN, use multiple usernames that don’t reveal your identity, don’t use an actual photo of yourself as your avatar, change your passwords regularly, and use two-factor authentication.

Gaming

Photo by Sean Do on Unsplash

Gamers or users with multiple accounts on video game enthusiast or streaming communities (i.e., twitch) are another likely set of doxxing victims.

You might remember the famous Gamergate, a harassment campaign against women in the video game industry, most notably the game developers Zoe Quinn and Brianna Wu.

However, playing video games can be dangerous, too. In 2014, a Canadian teen doxxed and swatted female gamers after they refused his friend requests and obscene demands. Swatting is when someone prank calls the emergency services in the hopes that they'll send armed police officers to a particular address.

Swatting can be deadly. In 2017, a gamer named Casey Viner asked a known "swatter" Tyler Barriss to make a fake emergency call to get back at a gamer in Wichita who had killed his in-game character in the game "Call of Duty: WWII." The address provided to the police turned out to be wrong, and an innocent man, unconnected to either gamer, was fatally shot.

What you can do to prevent doxxing: Opt-out of data brokers and people search sites, use a VPN to hide your IP address, and use different usernames and passwords across various sites.

Public-facing professions

Photo by Austin Neill on Unsplash

Famous people, like celebrities, presidential candidates, and successful business leaders, are also popular dox targets.

In 2013, hackers released the personal information of world-famous celebrities and politicians, like the rapper Jay Z, actor Mel Gibson, and former first lady of the U.S. Michelle Obama. The data exposed included phone numbers, home addresses, and social security numbers.

In 2015, Donald Trump doxxed Lindsey Graham on live TV. That same year, the then CEO of Turing Pharmaceuticals, Martin Shkreli, was doxxed after raising the price of the little-known drug Daraprim. Earlier this year, 38 police officers were doxxed during protests in Portland.

What you can do to prevent doxxing: Strengthen your passwords, use disposable contact details, and opt-out of data brokers.

Reporting

Photo by The Climate Reality Project on Unsplash

Journalists, especially those that cover controversial political topics, are faced with a high risk of doxxing, as well. Those that work on a freelance basis may be seen as easier targets because they don't have a support system (i.e.no HR department and similar). Moreover, their work address is usually their home address, and they typically send their tax documents over unencrypted email.

In 2013, the cybersecurity journalist Brian Krebs became one of the first reporters to become a victim of swatting. In 2014, the journalist Anna Merlan was doxxed after she criticized 4chan, a controversial online forum where users remain anonymous. In 2020, a New York Times journalist was doxxed after Fox News host Tucker Carlson said that The New York Times would reveal where he and his family lived in an upcoming story.

What you can do to prevent doxxing: Keep a different email address and phone number for work and personal use, encrypt email messages, and use a P.O. box instead of home address. If possible, consider using a pseudonym when publishing a controversial article and secure your social media accounts. Also, if you have a domain name, mask the registration information.

Activism

Racism is a Pandemic too!
BLACK LIVES Matter
TO IGNORE EVIL IS TO BECOME-ACCOMPLICE
"Stopping patterns must important to convince

Photo by Heather Mount on Unsplash

People that engage in activism are common doxxing targets, too. For example, members of the far-left group Antifa (anti-fascists) are often doxxed by far-right groups, as are individuals who attend “communist” protests.

Posting in the online community “Pony Power,” one neo-Nazi said, in response to Antifa’s counterprotest to “Say No to Marxism,” “So who is going to be there to stand up against Antifa? This is a good chance to dox them so we can have an idea of who they are. We should go onto their FB [Facebook] page if they have an active one and dox all the ones who plan on being there and who liked the post.”

However, you don’t need to belong to Antifa or go to a mass demonstration to get in trouble with neo-Nazis. Simply sympathizing with the far-left is, in most cases, enough.

One neo-Nazi, for example, shared a link to the Safety Pin Box, a “monthly subscription box for white people striving to the allies in the Black Liberation,” and suggested doxxing “white allies.” Another said they should doxx a girl who posted a photo of herself on Facebook wearing a t-shirt that said: “punch more Nazis.” And one neo-nazi even proposed doxxing "the liberal teachers of universities" because many Antifa members apparently come from liberal institutions.

What you can do to prevent doxxing: Tighten your social media settings (don't forget to turn off geotagging!), don't overshare online (i.e., don't tell people you're attending a specific event via Facebook), and don't bring your phone to protests. Also, use aliases when signing petitions, don't click on any strange links, and cover your face, scars, and tattoos when attending a rally.

Steps to Take to Prevent Doxxing

Photo by Christin Hume on Unsplash

Regardless of whether you're a gamer, journalist, or just someone who spends a lot of time online, the key to minimizing the risk of getting doxxed is reducing your digital footprint. To do this, don't post personal information online, secure your social media profiles, and remove yourself from data brokers.

That last step is vital. Data brokers have a ton of data on you, including your phone number, email address, and even information about your family. If a doxxer wants to find out where you live, all they have to do is google your name. Luckily, many data brokers let you opt-out of their databases. We have a detailed, step-by-step guide on how you can do that. Or, we can do it for you.

Crash Override Network, a site created by people targeted by GamerGate, has more tips on how you can protect your online identity.

What You Can Do If You've Already Been Doxxed

If the information exposed isn't particularly sensitive (or is already publicly available) and if you don't feel threatened, blocking the doxxer might be enough. However, if the information shared is sensitive or exposes you to harm, you might want to disable or delete your accounts and contact law enforcement.

Either way, make sure that you document all the evidence (i.e., take screenshots or download the page) as the initial attack may escalate quickly.

Most doxxers post people's private information on social media sites like Twitter or Reddit, which allow you to report abusive behavior.

If the dox includes your phone number, you'll probably want to change it. If the dox exposes your credit card number or other financial information, freeze your accounts. If the dox reveals your home address and you don't feel safe, go to the police and consider relocating, at least temporarily.

Life After Doxxing

Even if you've been doxxed, the most important thing is to stay calm. Doxxers crave attention, so your reaction will only spur them on. By taking the steps above, you can ensure your online and offline safety in the long run.

However, keep in mind that data brokers, the primary source of information for most doxxers, tend to relist people's profiles almost immediately after you opt-out. As such, it's vital that you monitor these sites continuously.

If that sounds like too much hassle for you, we'd be happy to help. DeleteMe is a subscription-based service that removes you from 40+ data brokers and people search sites — and keeps you off them for good.

Want more privacy news?

Join Incognito, our monthly newsletter from DeleteMe that keeps you posted on all things privacy and security.

First Name

Last Name

Email •