BIZ & IT —

Anti-doxing strategy—or, how to avoid 50 Qurans and $287 of Chick-Fil-A

Act before it's too late. Simple strategies *can* minimize the physical toll of doxing.

NATHAN MATTISE - 3/15/2015, 11:00 AM

Aurich Lawson / Thinkstock

Thanks to the Internet, old tricks get turned up in ease and volume.

"Nate, wake up. Your phone keeps going off."

This was two months ago—Monday morning, 4am—and I was asleep. But I remember what happened vividly. A decently hard nudge from my girlfriend did what technology couldn't, and I woke up to look at my phone. It showed two missed calls from unrecognized numbers alongside a slew of texts. I took a quick glance at the earliest unread message.

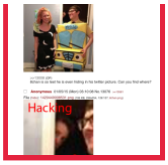
"Hey, 8chan has doxxed you," it read. "Message me on Twitter for more info."

Still in pajamas but now sitting on the couch with laptop in hand, I found the relevant thread. It began three hours earlier on the /baphomet forum of the anonymous message board 8chan. The first post said it all: "I am the hacker 8chan. Fear me, Nathan. I'm coming for your bunghole."

In addition to that cheerful welcome, my e-mail, phone number, current address, and social media profiles were all listed. Eighteen additional posts were already up, including:

> [1:48:31] I wonder how late places deliver in that town.
>
> [3:51:33] He looks high as shit in this picture. Also his last tweets were 8 hours ago. So he should be getting up in an hour or two. Journalist sleep schedule and all.
>
> [3:54:26] I also wonder if it's going to be a "The evil haxors are trying to silence me: But I CANNOT BE SILENCED" article.

That image is from my **Twitter profile**.



The next 14 hours became an on-and-off headache filled with phone calls, lawyers, and the local police. Gawker mentioned the incident, and at least nine pizzas were ordered to my address along with Qurans and other surprises. I had been doxed—my personal details were discovered, posted online, and then essentially used for harassment.

Let's pause for a moment. To address one of the anonymous posters above, no, this will *not* be an "evil haxors are trying to silence me" triumph of journalism tale. If you want that kind of story, there are plenty of examples elsewhere. While my day in the depths of doxing (or "doxxing" and "d0xing") was at times hellish and miserable, my encounter was a minor one on all fronts. I was targeted for writing a headline that upset 8chan users because it lazily used "8chan" to refer to a subset of the site's users. (The distinction was spelled out clearly in the opening paragraph, but there's obviously a premium on headlines today.)

Solid data on these kinds of incidents is hard to come by—onlineharassmentdata.org estimates 1 in 4 Americans has experienced online harassment; Pew says seven percent of the country has dealt with "sustained" periods of harassment. Anecdotal evidence certainly isn't encouraging. Back in 2013, security reporter Brian Krebs became an early journalism SWAT victim, but last year thousands witnessed such an attack happen in real time on Twitch. Others have had illicit images posted and used as blackmail in exchange for ransom money, and others still have experienced such sustained online harassment campaigns that an initial doxing is only the most minor of footnotes (especially when compared to physical death threats that impact one's life and career).

No matter the figures, the profile of online harassment has certainly risen. Doxing has been covered by mainstream press like *The Economist* or *New York Times*, and celebrities from Curt Schilling to Miley Cyrus to Lil Wayne have been involved in online harassment to varying degrees.

I'm not the only Ars staffer who's been doxed; I'm not even the most recent. But there seems to be a perceived increase in frequency for these incidents, so there's simply more interest than ever about what to *do* when something like this happens. While it's hard to say exactly how society at large needs to deal with the umbrella of online harassment—which includes everything from doxing to hate speech, SWAT attempts to stalking—we *can* think about concrete steps that may help people avoid Mondays like mine.

Your address

Maybe my doxing wasn't totally preventable; it's hard to say what a determined group of people can do with the Internet at their disposal. But there are tactics I could have taken earlier to better protect my information online, and there were actions I took to navigate the doxing as well as I could after the fact. The following observations, advice, tools, and other information are all general recommendations. Like online harassment as a whole, every doxing is different and may

require different responses. I was lucky enough to encounter a situation where no direct hacking occurred, and this piece reflects that.

(*Note:* While someone who wants to complicate your life can obviously do far more damage with passwords or access to various bank, e-mail, cloud, or other accounts, that's not *necessary* to implement an infuriating doxing or worse. Keep in mind the cautionary tale of then-*Wired* writer Mat Honan. A little bit of information and a lot of social engineering can go a long way.)

When I saw the post broadcasting my information to who knows how many, it appeared to be a screenshot of a copy/paste job into some basic text editor. Since I'm a journalist, even your most infuriatingly tech-challenged relatives could likely find my e-mail and phone number. What worried me was the address. Phones can be turned off, Twitter handles made private, e-mail addresses changed. The most worrisome aspect of a doxing is the potential for it to physically manifest at your home.

I immediately checked various online accounts searching for any hint of intrusion. *Nothing.* I double checked that I didn't foolishly include this info on some old resume or on LinkedIn, but those were clean. Social profiles only pointed to New Orleans if they displayed a location at all, and I'm a stickler for turning off GPS sync with most services. It was only later that I realized the likely source—the order of the information posted matched verbatim what someone might find through a particularly easy kind of online search.

Enlarge / My "beautiful" website, not worth being doxed for. (Yes, created in Dreamweaver, probably in CS 3.)

whatis a whois

If I had thought of it earlier, I could have made life a bit harder on my doxers. Most of us are smart enough to keep social network profiles either private or scant of important personal or contact information (and if you don't already, do going forward). But there are legitimate services that may be storing these details in plain sight, and even a relatively basic Internet user can access them through a simple Web search.

For instance, do you own a domain? ICANN, the non-profit responsible for unique identifiers across the Internet, requires every domain registered to have publicly listed contact information (with different top-level domains having different rules for how and how much information must be displayed). And while there was debate in 2013 (PDF) about making that data less public (accessible only in situations like legal cases or purchases and sales), today anyone can use publicly available online tools to find this whois information for any domain. For example, a whois lookup on arstechnica.com shows you who owns it (Condé Nast Digital) as well as the administrative and technical contacts.

So if you've registered a domain, the information you provided may be similarly visible—clearly not an ideal situation when guarding against online harassment. You may *think* the answer here is simple: don't provide some details (address, phone number, primary e-mail, etc.) or provide fake details. However, depending on the hosting service, your *billing* information may double as your ICANN information. From personal experience, the popular Hostmonster is one such outlet. Even after updating official "contact information" through the service post-dox, a simple whois search produced the original information more than a month after the fact.

Instead, the real solution is simple yet frustrating: pay up. Most registrars sell a service variously called "WHOIS protection," "Privacy Guard," or other similar names, an offering where they substitute their own information into ICANN's database instead of yours. At Hostmonster, $12 per year will swap out any personal details via the Hostmonster Domain Privacy service. Other registrars (like Gandi.net) offer such services for free.

Page: 1 2 3 Next →

NATHAN MATTISE

Nathan is an Austin-based Features Editor at Ars Technica. He edits and contributes posts on a variety of topics like lost short films that ran before *Empire*, how NASA kept the Shuttle program going against Hurricane Katrina, and why Apple no longer loves indie bands. He also hosts and produces Decrypted, Ars Technica's Mr. Robot podcast.

EMAIL nathan.mattise@arstechnica.com // **TWITTER** @nathanmattise

READER COMMENTS 137 SHARE THIS STORY

← PREVIOUS STORY NEXT STORY →

Related Stories

Sponsored Stories

Powered by

Today on Ars

RSS FEEDS
VIEW MOBILE SITE
VISIT ARS TECHNICA UK
ABOUT US
CONTACT US
STAFF
ADVERTISE WITH US
REPRINTS