What To Do If You Are Doxx'd by Trolls Documentation

Release 0.1

Various

March 13, 2015

Contents

Or, *What to Do If You've Been Doxx'd by Trolls* [1]

This guide is an resource for victims (and their families and support network) of online harassment, trolling, and particularly *DOXXing*. Its creation was inspired by the events surrounding GamerGate and the brutal online abuse of Anita Sarkeesian, Zoe Quinn, Brianna Wu, and Randi Harper, but it is dedicated to everyone enduring this immature, toxic and destructive Internet culture.

[1] From Adria Richards' tweet series, "If trolls have doxx'd you".

CHAPTER 1

About This Guide

This resource is being compiled over time from various sources, as a way to help victims of online abuse and harassment protect themselves and their families. This project was inspired by Adria Richards' series of Tweets, "If trolls have doxx'd you" (embedded below).

1.1 The Storify

CHAPTER 2

1. Reporting Threats of Violence

Step 1: If you are receiving threats of violence, *do not hesitate to report them to the appropriate authorities*. Even if nothing comes from it immediately, it is wise to have an incendent report and case number if things escalate. Harassers will intimidate and dismiss reporting threats as "hysterics" – *ignore them and report the threats*.

2.1 Government Authorities

2.1.1 Local Police

Don't call *911* (or your local equivalent emergency number) unless there is an immediate physical threat; call the main station number. You might be asked to request your private data from Twitter and other social media:

- Twitter, Guidelines for Law Enforcement
- Facebook, Information for Law Enforcement Authorities. See "User Consent" for information on where to download your information

2.1.2 National

The FBI, also the Internet Crime Complaint Center.

2.2 Social Media

Twitter's Abusive User report form

Caveat:

Twitter will not (as of this writing) review threat reports from third parties:

WAM and Twitter

Women, Action and the Media has created a reporting form where you can report harassment, threats etc on Twitter. These reports are checked by a human and then passed on to Twitter:

> Just use the form below to tell us what's happening. If it checks out, we'll escalate it to Twitter right away (24 hours max, hopefully much less than that) and work to get you a speedy resolution. But please note: we're not Twitter, and we can't make decisions for them. We're going to do our best to advocate for you with them, though.

CHAPTER 3

2. Who To Notify

In addition to online "verbal" abuse, threats and harassment, victims of *doxxing* are also at risk of offline harassment and identity theft which can result in real financial and reputational damage. When researching a user during a doxxing, that user's Social Security Number(SSN) can often be discovered. While this identifier was never intended to become a universal identifier for business and commerce, knowing this vital bit of information plus personal details researched from a variety of sources can somtimes help attackers gain access to otherwise secure accounts (see notes on Spokeo, a site popular with identity thieves and hackers).

Notifying the authorities and employers, financial institutions, and service providers **quickly** and **clearly** can help reduce the damage footprint.

3.1 Authorities and Employers

- Call your local police department (not 911), give them your address and ask them to watch for potential fake calls/reports (called *SWATting*)
- Your employer. Victims have been let go from positions after bogus complaints/reports were called in by harassers. Let your employer know that this is happening and... (?)

3.2 Banks

Contact your bank via the identity theft or fraud departments, and inform them what's happening and request a *safe word* on the account.

- Bank of America identity theft
- Wells Fargo identity theft
- Chase Bank Security - Fraud reporting (also accountatrisk@chase.com)
- CitiBank identity theft

3.3 USPS

- US Postal Inspection Service identity theft reporting page

3.4 Credit Cards/Credit Bureaus

Start with the credit bureaus: The FTC has a guide on how to Place A Fraud Alert with one of the major credit bureaus.

> "Ask 1 of the 3 credit reporting companies to put a fraud alert on your credit report. They must tell the other 2 companies. An initial fraud alert can make it harder for an identity thief to open more accounts in your name. The alert lasts 90 days but you can renew it." [FTC]

The guide has a helpful checklist to follow.

3.5 Medical Providers

3.6 Cell Provider

Reporting fraud/identity theft:

- AT&T, Fraud Protection and Prevention
- T-Mobile, Identity Theft (basically, see the FTC)
- Verizon, Fraud Prevention
- Sprint, Clearing up identity theft (looks to be a hassle)

3.7 Internet Provider

Sources

3. What To Change/Secure

When you are being harassed, or if you've been doxxed, there is a long list of things you can do to secure your digital life and reduce the impact that harassers can have.

Read all of Zoe's post, "What To Expect When You're Expecting (the internet to ruin your life)" [ZQ1]

4.1 Passwords

Change Passwords. **Change Passwords**. One more time: **Change Passwords**.

Think about how passwords are handled.

Use a password manager like 1Password or Lastpass, set passwords to more-than-8 characters, randomized with upper and lower-case and numbers/punctuation.

4.2 Account Security Questions

> Zoe Quinn: "Change your security questions to something that isn't related to your personal life." [ZQ1]

4.3 Email

> If you aren't using Gmail consider starting. Google provides access over SSL (ie, HTTPS, use it) and it means your email is not sitting on your harddrive waiting to be hacked or stolen with your laptop.

4.4 Enable 2factor Everywhere

Two-factor authentication means needing more than simply a password to login to any account where it is enabled.

> John Seggerson: "The idea is having not only a fixed password to log in (one factor), but a code which is either given to you or using a secret algorithm to generate a one-time code (second factor)." [SM1]

Two Factor Auth (2FA) - List of websites and whether or not they support 2FA.

Lifehacker also has a good article on enabling and using 2-factor authentication.

4.5 Spokeo

Remove yourself from Spokeo: Spokeo crawls publicly available information (including website profiles) about individuals and makes it completely searchable online by the individual's name. This information includes current and previous addresses, phone numbers and other contact information. Trolls can and do use this data to fuel harasssment campaigns.

> John Sileo: "Go to the [Spokeo] and look yourself up, then click on your name... once you have done that copy the URL in your web browser. Now, go to the bottom right of the page in small faded blue text, click privacy (third from the left). Once done, paste in the link you copied from the page you found yourself on and enter your email and the security code listed. This is a case where I would use a second email account (your designated junk-email account), not your main email to avoid the build up of possible spam emails that follow. It will then send you an email confirmation where you must click the URL to confirm removal. Voila! You have been removed."

Spokeo – Scary Bad & How to Opt Out [SIL1]

4.6 Social Media Sites

> Zoe Quinn: "Make your FB private. They will likely be trying to dig up whatever they can on you, real or imagined, and there's no reason to leave stuff out there when you're being creepily obsessed over. Make sure old posts get limited too - go to settings > privacy > limit past posts to do this." [ZQ1]

4.7 Storage accounts (iTunes, Dropbox, Skydrive)

4.8 EXIF/Photos

> Turn off or remove *EXIF* data from your photos, if you are still posting.
>
> Uncommon Privacy: "Exif data contains a number of metadata tags about the photo such as the date and time it was taken, make and model of the camera, various camera settings and other information including GPS information. Exif data is a risk because by sharing photos over the internet, you may be revealing personal information such as where you live, where you work or where your children go to school." [UP1]

4.9 Domains

> Zoe Quinn: "Spend the $10 to hide your whois info off of your websites ahead of time if you can. This is a very common tactic." [ZQ1]
>
> Any blog or site where a victim publishes is a likely target for *DDoS* ing or defacement. It is especially important to enable *whois* privacy for all owned domains, as a harasser can use a service like Bing's IP lookup to find all domains hosted on a given IP address.
>
> 1. Ping `yourblogdomain.com` to get an IP address `1.2.3.4`
> 2. Search `ip:1.2.3.4` on Bing to get results for sites/domains with the same IP address `yourbusinessdomain.com`
> 3. Target `yourbusinessdomain.com` as well for attack.

Sources

A majority of this material was written with input from victims of harassment or compiled from personal reports.

CHAPTER 5

4. What To Tell Friends and Family

When being doxx'd, attackers may use that personal information to contact family members and/or friends and use that information to get them to divulge more details of your life (*social engineering*). Attackers may also contact family members to simply harass, make accusations against the victim, or threaten the family. It is important to (selectively) let family know what is happening, that they don't have to freak out (even though it certainly feel appropriate), and give them tips on not engaging:

> Zoe Quinn: "Give other people affected a heads up & make sure they don't give out more info. For example, in my case they spammed my former employers dating back all the way to when I was a teenager, trying to dig up more info on me. I know it can suck to have to try and explain this stuff to people, but it can keep more information from leaking out. Similarly, try to make sure people don't freak out, and that they shouldn't engage with these people or do anything other than hang up." [ZQ1]

It's also important to inform family and friends that are active on social media that it's possible that fake accounts might be started with your name/avatar on them. Make sure they check with you via another channel before reacting/responding to outlandish or out-of-character posts seemingly from you.

5.1 How Family/Friends Can Help

Ashe Dryden:

> "In the event of really shitty things going down, I will reach out to a couple people that I trust to help me screen twitter, emails, and any things else necessary. If we are friends and you are worried, contact the people closest to me and they will be the best ones to give you updates so I don't get overwhelmed." [AD1]

5.1.1 Twitter Tips:

[Ed.] If you are defending a victim on social media, think about removing their @username from the threads, so that you "draw fire" and help clear their timeline of unwanted communication.

Ashe Dryden:

- **block/report for spam** the people in my mentions that are being harassing
- **take a screenshot and document** any information available (URLs, handles, names, etc) if it is a physical threat or if it would violate the twitter TOS so that I can report them as abuse through Twitter if it gets to that
- **do not reply to trolls or harassers** with my name in the tweet. If I have stopped engaging with a person, take that as a sign that I don't want to see anything related to them either. If I have to ask you more than once to stop replying to me with their info attached, I may have to block you.

- **don't reply to them with a period before their handle**; I don't want to see it in my timeline.
- **don't use a hashtag we've created** when replying to their trolling, harassment, or threats as this may trigger other people. [AD1]

Sources

CHAPTER 6

Tools

6.1 Handling Twitter

GoodGame Autoblocker (GamerGate block list)

Specific to the trolls harassing women in gaming and their supporters, the ggautoblocker list on BlockTogether will block over 7000 twitter accounts who have been algorithmically determined to be GamerGate supporters. (Block list on BlockTogether)
(created by Randi Harper)

https://blocktogether.org/

> "An app intended to help cope with harassers and abusers on Twitter. When you sign up for Block Together, you can view a list of your own blocks. You can also use the auto-block and block sharing options listed below."

6.2 2-Factor Auth tools

- Duo Mobile is a great, easy to use authenticator app with mobile clients.

6.3 Privacy Resources

- EPIC (Electronic Privacy Information Center) Privacy Tools
- Pipl See what's publically available about you based on name or email address.
- Woodycraft.net: How To Prevent Yourself From Being Dox'ed

6.4 Documentation

Zoe Quinn, 'What To Expect When You're Expecting (the internet to ruin your life

> "It's better to have it and not need it than not have it and need it. If you end up needing to take it to the authorities, they're gonna wanna see this stuff, and the more you have the better." [ZQ1]

- http://archive.today/

WHO@:

> "Save everything: One of the first impulses many harassment victims have is to just delete any communications they've received, and that's a bad idea. It's important to save absolutely every communication you have with the harasser - email, chat logs, ICQ histories, anything. If the harasser has created a web site about you, save copies of it to your local system and have someone you trust who would testify in court for you if necessary to do the same. If you receive any phone calls from the harasser, have them traced immediately (your local phone company can tell you how to do that). If you receive any kind of postal mail or other offline communications, save them (with envelopes, boxes, etc.). Do not destroy any evidence - and do not handle it more than absolutely necessary or permit anyone else to do so. Immediately turn the evidence over to the police. Place envelopes, letters, etc. in plastic bags to protect any possible fingerprints." [WHO1]

6.5 Password Generators

- 1Password - Mac, iOS , Windows, Android password manager and generator. Can generate and store randomized passwords for most any website, iTunes account, email account, and many others.
- (others?)

Sources

CHAPTER 7

Self Care

Zoe Quinn:

> "Don't give yourself a hard time for feeling a certain way. It's a messed up position you've been put in and there's no 'right" way to feel. You're not failing if it bothers you, you're not failing if you're angry, you are not failing for not being "tough enough". A lot of emotions come with these situations, and you're totally allowed." [ZQ1]
>
> "Don't suffer alone. Make sure you reach out, and again, don't judge yourself. It's not weak to want or need help or to vent. There are so many women in the industry who understand what you're going through and would be happy to help however they can. If you have someone in person that can look after you, all the better. They'll remind you that what is happening to you is wrong, they will help make sure you're taken care of, and it's a huge huge asset." [ZQ1]

Sources

CHAPTER 8

Prevention

8.1 Defense Against The Doxx Arts

Computer World:

> Unfortunately, doxxers don't have to work very hard to find a victim's personal info. A number of free and paid services known as data brokers create profiles of vast numbers of individuals based on aggregated data from business directories, social media and other public records. With a specific target in mind, all a doxxer has to do is search one or more of these services to find the details he or she wants."

8.2 Resources

- Uncommon Privacy, What is doxxing?
- Uncommon Privacy, How to Keep Yourself from being Doxxed
- Working to Halt Online Abuse, Staying Safe Online

CHAPTER 9

Glossary

DDoS Distributed Denial of Service attack - a website attack that uses large numbers of distrubuted agents (a botnet usually) to send massive amounts of website traffic, usually overloading and crashing the website's server and bringing it offline.

doxxing From *dox*, for *documents*. Finding and publishing documents with personal (but public) information about a target.

"Doxing consists of aggregating as much information on an individual or organization using social media networks, web search engines, social engineering, basic deduction skills, and password cracking methods...

Once enough information is gathered on a targeted individual or organization, the attacker openly publishes the target's personal photos, personally identifiable information, and any other information, including information on family members, in retaliation for a perceived offensive action the target or the target's organization may have taken." [NORRIS]

EXIF Digital image data stored in image files by cameras, scanners, smartphones and computers. Often includes time, date, and exact geographic location the photo was taken.

SWATting "Swatting is the tricking of any emergency service (via such means as hoaxing a 9-1-1 dispatcher) into dispatching an emergency response based on the false report of an on-going critical incident" [WIKI2]

Whois "WHOIS (pronounced as the phrase who is) is a query and response protocol that is widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block" [WIKI1]

Sources

CHAPTER 10

Doxxing

There are many forms of online harassment, trolling and abuse - but perhaps the most frightening abuses come in the form of *DOXXing*: posting (often publically available) personal information online for the purpose of creating embarassment and/or fear in the victim, enabling others to pursue more dangerous forms of harassment, and ultimately to silence the victim by driving them from public life.

> The Economist: "The term "dox" (also spelt "doxx", and short for "[dropping] documents") first came into vogue as a verb around a decade ago, referring to malicious hackers' habit of collecting personal and private information, including home addresses and national identity numbers." [ECON1]
>
> "Typically, as is the custom of those who find pinching and compiling personal information a viable alternative to team sports, it will be released in a massive 'blast' post on some obscure message board and linked to on a popular forum" [CPAC1]
>
> "The problem is, they may actually have something on you if they're a dedicated group willing to spend lots of time posing as a long-lost BFF or that one girl you met that one time down by the wharves. What am I talking about? (And what were you doing down by the wharves?) I'm talking about social media–like facebook, or twitter. If you use them a lot, you'll probably have your name and location listed publicly, or a friend or family member will. There are a lot of 'John Smith's in the world, but if they've got a John Smith who lives in Vancouver, Washington, and you've listed yourself as John Smith of Vancouver, Washington, the pieces start to come together." [CPAC1]

The information discosed in a doxxing can and does lead to more destructive harassment, information or identity theft, financial and career damage... the list is long and terrifying.

> "Now they've got something on you, and depending on how lax your security is, they may be able to go through your life and find the answers to your password security questions like "name of first pet" or "mother's maiden name". From there, it gets really hard to tell where the problems will stop..." [CPAC1]

This (incomplete but regularly updated) guide is intended to help navigate this frustrating, frightening - and infuriating - situation.

Sources

[FTC] The FTC, Place a Fraud Alert

[ZQ1] Zoe Quinn, What To Expect When You're Expecting (the internet to ruin your life)

[SM1] John "Seg" Seggerson, The Quick Indie Guide To Protecting Your Accounts

[SIL1] John Sileo, Spokeo – Scary Bad & How to Opt Out

[UP1] Uncommon Privacy, How to Remove Exif Data From Photos

[ZQ1] Zoe Quinn, What To Expect When You're Expecting (the internet to ruin your life)

[AD1] Ashe Dryden, Trolling, threats, and abuse: how you can help me

[ZQ1] Zoe Quinn, What To Expect When You're Expecting (the internet to ruin your life)

[WHO1] Working to Halt Online Abuse

[ZQ1] Zoe Quinn, What To Expect When You're Expecting (the internet to ruin your life)

[WIKI1] WHOIS, Wikipedia

[WIKI2] Swatting, Wikipedia

[NORRIS] Mitigating the effects of Doxing, 2012

[ECON1] The Economist, What doxxing is, and why it matters

[CPAC1] So You've Been Doxed...