Doxxing: Inevitable or avoidable?

Eliza Schreibman

Mentor: Ming Chow

Fall 2015

**Abstract**

Over the past two decades, billions of people have become comfortable with treating the Internet like a second home. Many, if not most, of these people take for granted how the Internet works and how secure (or not) their communications and information really are. Various security issues have challenged this comfort, from password cracking to database breaching, but there is one particularly unnerving issue that has stormed into the limelight over the past couple of years: doxing. Doxing is so dangerous because it is so easy to execute, hard to avoid, and personalized in its targeting; doxing has arguably the greatest potential for not only physical or monetary harm to its victims but also lasting psychological trauma. Here we will not only investigate doxing methodologies and preventative measures, but ultimately decide if it is even possible to avoid being a doxing victim.

**To the Community**

While I am not here to claim that doxing is inherently an evil methodology—in fact I will later discuss some cases of “hacktivist” doxing—we need to talk about the dark and ugly consequences of doxxing[[1]](#footnote-1). While it is certainly not the only example, GamerGate[[2]](#endnote-1) might be the epitome of doxing can be used to harass, threaten, and nearly destroy people’s lives. Doxers involved in GamerGate have obliterated any chance at normalcy for some prominent female game developers and game critics such as Zoe Quinn[[3]](#endnote-2), Brianna Wu[[4]](#endnote-3), and Anita Sarkeesian[[5]](#endnote-4). All three women have stood up and condemned all forms of harassment, but disgusting and violent comments are only the tip of the iceberg. All three women have had to leave their homes at some point after their addresses were leaked through doxing; all three have had family and friends around them doxed as well; all three work in the tech industry, meaning they don’t have the option of going of the grid if they want to continue their work. And they are not the only ones: there are countless other people, most often women, people of color, and LGBT folks, whose lives have been shaken if not ripped apart because of doxing. What’s even scarier, as I will detail later on, is how easy it is to dox someone and how hard it is to hide your personal information and prevent attackers from building a complete profile of your life. Plus there is the added dark irony that legal repercussions are all but non-existent for attackers, despite the fact that all the threats and information posts are publically available. I don’t envision doxing going away anytime soon, and, as an outspoken queer woman in the tech industry, this terrifies me. That is why I chose this topic: to educate, investigate, and arm others and myself with information about doxing so that maybe someone can avoid this kind of calamity.

**Introduction**

Doxing (alternatively doxxing) is an attack method by which a group of people, or sometimes an individual, seek out publically available information on their target (often connecting simple information such as a name or hometown to more personal information such as bank account passwords) and then post that information across various sites in the hopes of shaming, angering, or scaring the target.[[6]](#endnote-5) The four cornerstones to doxing are the mob mentality/hive mind of the attackers, the fact that the information is publicly available, the ability to connect information and build a detailed profile of the victim, and the fact that these attacks are motivated by wanting to harm to the victim (with no benefits or gains to the attackers). Attackers vary widely from case to case, but two of the most well known groups who have claimed responsibility for numerous high-profile doxings are the supporters of GamerGate and Anonymous. The act of doxing, unlike sneaky researching or stalking, is most often executed in a very vocal manner (e.g. attackers announcing who they are attacking, what information they plan on exposing, etc.) by posting information on twitter, reddit, 8chan, or pastebin. Additionally, “really big problems come when someone connects all of the dots and builds up a profile that covers all aspects of your life.”[[7]](#endnote-6) Finally, attackers’ main goal is not to expose information for the sake of exposure or even to expose credit card information in the hopes of buying themselves things; in fact, in one relatively harmless case, a man’s credit card information was doxed and used to send him 50 Qurans and $287 of Chick-Fil-A.[[8]](#endnote-7) These factors all combine to make doxing an extremely powerful tool that can be wielded by anyone. It’s also a tool, one might argue, that it isn’t inherently evil; in fact, many point to cases such as the Anonymous doxing of some Missouri KKK members[[9]](#endnote-8) or alleged ISIS recruiters[[10]](#endnote-9). Others counter that Anonymous has doxed innocent people (accidentally[[11]](#endnote-10) and maliciously[[12]](#endnote-11)) and, as discussed earlier, there are harassment groups such as GamerGate who have used doxing to devastate their victim’s lives. I mention these cases not to debate whether or not Doxing is good, bad, or evil but rather to highlight the breadth, depth, and diversity that goes into doxing.

Now that we understand the mentality of a doxer, we will dive deep into their methods and tools for finding information as well as how you can prevent, detect, and minimize damage from doxing.

**Doxing Attacks**

***Common Attacks***

One of the reasons doxing is so powerful is because the majority of attacks require very little technical skill and are mostly free. These attacks have two main components: gathering as much data as possible and then creating a web of information from that to access more sensitive information. Much of this can be accomplished through a combination of social engineering and persistence. In this first step, attackers are looking for everything and anything, and they are usually going off of only a small snippet of information such as a username.[[13]](#endnote-12)[[14]](#endnote-13) Throughout my research, the most common items that were sought out were: full name, age, picture, usernames, social media accounts, email, phone number, and personal details[[15]](#footnote-2). Most of this can be found through a little digging on various search engines (e.g. Google, Bing, Yahoo). After that preliminary search, attackers will then look into search engines that are designed to find information about people such as Spokeo[[16]](#endnote-14), Whitepages[[17]](#endnote-15), and Pipl[[18]](#endnote-16). Additionally, attackers may repeat this steps on the victim’s family or friends to gain further leverage. These pieces of information are good for two purposes: building a profile and spam harassment. Some common types of spam harassment include text or sms bombing[[19]](#endnote-17) and unwanted Skype calls, Facebook messages, tweets, Skype calls, or emails[[20]](#endnote-18).

Remember that doxing is usually a group operation, so together a group will be able to collaborate and share information faster and with greater detail than just a single individual. Once enough information is collected, attackers begin on the more important and scary phase: getting personal information. This includes: IP address, passwords, credit cards, bank accounts, social security number, medical history, and home/work address. This information is particularly lethal, since it could lead to someone causing the victim physical harm. MAC and IP addresses are fairly easy to find; attackers can use the target’s website or email address. Attackers can use the UNIX commands ping, lookup, traceroute, and finger to get the IP address of a given website.[[21]](#endnote-19) Similarly, if any attacker has an email sent from the victim, you can use various sites to read the email’s full header to find the source IP address.[[22]](#endnote-20) Once an IP address is acquired (assuming this is the victim’s actual IP address), a quick lookup of the location can be found on places like iplocation.[[23]](#endnote-21) Cracking passwords can be done in a variety of ways as well. You can combine brute force password cracking (with tools such as John the Ripper or Hashcat) with some social engineering. Most sites now have an “I forgot my password” button or something that asks the user to answer a security question; many of these questions (e.g. mother’s maiden name, first pet name, etc.) can be answered with information gained earlier in the doxing process. If any of these passwords happen to be a master password to a password manager such as site such as Last Pass or 1Password, this could potentially unlock credit card information and passwords to online health sites (e.g. Blue Cross Blue Shield, Atrius Health, etc.) or online banking services (e.g. Bank of America, Chase, etc.). Having any of this information posted or used against you is a huge threat that would involve a large amount of clean up, as we’ll discuss later. But what might be even scarier are attackers finding your home or work address. If the victim owns a domain name, they are required to have resisted and publicly listed contact information, which often contains a physical address; this information can be found on sites like whois[[24]](#endnote-22), 411 and whitepages.[[25]](#endnote-23)

***Advanced Attacks***

While a huge amount of damage can be done with the common attacks described above, it is worth mentioning a few other attack methods that are more technically advanced or require the attacker to be in close physical proximity to the victim. A few of these techniques rely on being on the same network as the victim. Packet sniffing, the process of looking at all the traffic on your network with the potential of accessing information in the clear,[[26]](#endnote-24) is one possible way to steal unencrypted data. Another possibility is creating a fake wireless access point; this technique is rare for doxing because it not only requires the attacker to be in the same location as the target but also they need to get the target to use the fake WAP, which requires some further social engineering. Other techniques involve compromising the victim’s computer or database to gain information. This can include things such as the bait and switch, whereby the victim thinks they are downloading a harmless file but it is switched out for a malicious one, or changing file names or file extensions to dupe the victim into downloading nasty software.[[27]](#endnote-25) Additionally, an attacker could go so far as to break into a victim’s database via SQL injection or cross-site request forgery. Again, these methods are not common, but they are important to discuss since they highlight how vulnerable we are and how often we take things such as the safe transfer of sensitive information for granted.

**Doxing Defenses**

***(Realistic) Prevention Methods***

***Defense and Damage Control***

How are people most commonly doxed

Doxing involves two main processes

Gathering large amounts of data

Trying to find as much information as possible

General information (name, age, picture, birthday,)

Personal/deeper information (information on family members/friends, deadname, SSN)

Usernames/Email

Phone number

IP Address

Passwords

Financial Information

Home address

Online search tools

Mostly just brute force finding every scrap of information

General search engines (Google, Bing, Yahoo)

Personal information websites (Spokeo, Whitepages, Pipl, Whois)

Connecting the dots

Using information easily found (birthday, mother’s maiden name, hometown) to get more secure information (email/username access, bank account)

Trying to find the most personal information that threatens a victim’s physical, financial, or emotional well-being

One of the following:

Action Items - In your own words, what do people need to do about the subject matter?

Defenses - Recommended if you work is attack-oriented. In your own words, how do you defend against the subject matter?

Applications - Recommended if your work is more theoretical. In your own words, how can you apply your subject matter to the real world?

Prevention, detection, clean-up

Prevention

Limit what information you put on the internet

Think about not just individual pieces of information but most importantly how they connect with each other

Two-factor authentication

Login attempt alerts

Financial limitations

Password manager/creator (Lastpass, 1Password)

Use a VPN TOR to mask your IP address

Google voice (creates a phone number not bound to your physical phone)

Detection

Honeypot

Scanning for attackers trying to log into your accounts

Clean-up after an attack has begun/occurred

Change emails/phone numbers/passwords

Freeze accounts (skype, social media, banks)

Emotional support

Use the publicity and hive mind against them: monitor and see them brag or laugh about what misery they are trying to infect upon you so that you can detect it and stop it (50 Qurans article)

**Conclusion or Summary**

**Conclusion**

Doxxing is fast, easy, and extremely damaging

Not just about how much information is out there but how it connects

Anybody can be a target, but certain groups are attacked more often

Prevention methods exist, but they are not perfect

Need stronger privacy law and a cultural shift

**References**

Articles:

<http://www.jonjones.com/2014/10/02/gamergatesurvivalguide/>

<http://onlineharassmentdata.org/>

<http://arstechnica.com/tech-policy/2014/08/popular-gamers-real-life-swat-raid-livestreamed-on-twitch/>

<http://www.computerworld.com/article/2849263/doxxing-defense-remove-your-personal-info-from-data-brokers.html>

<https://ctrlaltnarwhal.wordpress.com/2012/10/21/how-to-dox-anyone/>

<http://www.dailydot.com/politics/dox-doxing-protection-how-to/>

<http://null-byte.wonderhowto.com/inspiration/dont-get-doxed-5-steps-protecting-your-private-information-web-0133806/>

<http://www.infoworld.com/article/2610239/malware/7-sneak-attacks-used-by-today-s-most-devious-hackers.html>

<http://www.bustle.com/articles/63466-im-brianna-wu-and-im-risking-my-life-standing-up-to-gamergate>

Tools/sites using:

<https://www.reddit.com/r/technology/comments/j1mit/how_to_remove_yourself_from_all_background_check/>

<https://support.microsoft.com/en-us/skype?language=en&locale=EN-US&oaspworkflow=start_1.0.0.0&needslogin=false&wfname=skype&ccsid=635821634221835582>

<http://aruljohn.com/info/howtofindipaddress/>

<http://www.wikihow.com/Trace-an-IP-Address>

<http://www.spokeo.com/>

<http://www.whitepages.com/>

<https://pipl.com/>

**References**

1. Please proceed with caution when investigating the cited articles surrounding GamerGate, as many of them have screenshots and quotes from harassers which some might find upsetting or triggering. [↑](#footnote-ref-1)
2. Dewey, Caitlin. "The Only Guide to Gamergate You Will Ever Need to Read." *Washington Post*. The Washington Post, 14 Oct. 2014. Web. 14 Dec. 2015. [↑](#endnote-ref-1)
3. Parkin, Simon. "Zoe Quinn's Depression Quest - The New Yorker." *The New Yorker*. 9 Sept. 2014. Web. 14 Dec. 2015. [↑](#endnote-ref-2)
4. Wu, Brianna. "I'm Brianna Wu and I'm Risking My Life Standing up to GamerGate." *Bustle*. 11 Feb. 2015. Web. 14 Dec. 2015. [↑](#endnote-ref-3)
5. Robertson, Adi. "Trolls Drive Anita Sarkeesian out of Her House to Prove Misogyny Doesn't Exist." *The Verge*. 27 Aug. 2014. Web. 14 Dec. 2015. [↑](#endnote-ref-4)
6. Ramesh, Srikanth. "What Is Doxing and How It Is Done?" *GoHacking*. Web. 14 Dec. 2015. [↑](#endnote-ref-5)
7. Cox, Joseph. "I Was Taught to Dox by a Master." *The Daily Dot*. 6 Jan. 2015. Web. 14 Dec. 2015. [↑](#endnote-ref-6)
8. Mattise, Nathan. "Anti-doxing Strategy—or, How to Avoid 50 Qurans and $287 of Chick-Fil-A." 15 Mar. 2015. Web. 14 Dec. 2015. [↑](#endnote-ref-7)
9. Smith, S.E. "Anonymous Is Doxing KKK Members (and I'm OK with It)." *The Daily Dot*. 17 Nov. 2014. Web. 14 Dec. 2015. [↑](#endnote-ref-8)
10. Dunn, Matthew. "How Anonymous Could Bring down Islamic State." *NewsComAu*. 16 Nov. 2015. Web. 14 Dec. 2015. [↑](#endnote-ref-9)
11. Price, Rob. "All the times Anonymous Outed the Wrong Person." *The Daily Dot*. 19 Aug. 2014. Web. 14 Dec. 2015. [↑](#endnote-ref-10)
12. Vankoot, Bex. "It Happened to Me: I Got Doxxed by Anonymous." *Xojane.com*. 15 Jan. 2015. Web. 14 Dec. 2015. [↑](#endnote-ref-11)
13. "How to Dox Anyone." *Ctrlaltnarwhal*. 21 Oct. 2012. Web. 14 Dec. 2015. [↑](#endnote-ref-12)
14. <https://www.facebook.com/permalink.php?id=376357029151762&story_fbid=376361642484634> [↑](#endnote-ref-13)
15. For female targets, this is often sexual history, weight, etc. For people of color this is often their race, ethnicity, or birthplace. For LGBT folks, this is often sexuality, dead name, [↑](#footnote-ref-2)
16. <http://www.spokeo.com/> [↑](#endnote-ref-14)
17. <http://www.whitepages.com/> [↑](#endnote-ref-15)
18. <https://pipl.com/> [↑](#endnote-ref-16)
19. Mattise, Nathan. "Anti-doxing Strategy—or, How to Avoid 50 Qurans and $287 of Chick-Fil-A." 15 Mar. 2015. Web. 14 Dec. 2015. [↑](#endnote-ref-17)
20. "So You’ve Been Doxed: A Guide to Best Practices." *Crash Override Network*. 21 Mar. 2015. Web. 15 Dec. 2015. [↑](#endnote-ref-18)
21. <http://www.wikihow.com/Trace-an-IP-Address> [↑](#endnote-ref-19)
22. John, Arul. "How to Find the IP Address of the Email Sender in Gmail, Yahoo Mail, Hotmail, AOL, Outlook Express, Etc." *Aruls*. 15 Dec. 2010. Web. 14 Dec. 2015. [↑](#endnote-ref-20)
23. <https://www.iplocation.net/> [↑](#endnote-ref-21)
24. <https://www.whois.net/> [↑](#endnote-ref-22)
25. Mattise, Nathan. "Anti-doxing Strategy—or, How to Avoid 50 Qurans and $287 of Chick-Fil-A." 15 Mar. 2015. Web. 14 Dec. 2015. [↑](#endnote-ref-23)
26. Chow, Ming. "COMP 116: Introduction to Computer Security." *- Networking and Attacking Networks*. 15 Sept. 2015. Web. 15 Dec. 2015. [↑](#endnote-ref-24)
27. Grimes, Roger. "7 Sneak Attacks Used by Today's Most Devious Hackers." *InfoWorld*. 30 Sept. 2013. Web. 15 Dec. 2015. [↑](#endnote-ref-25)