Doxing Methodologies and Defenses: The Inevitable (or Avoidable?) Plastering of Sensitive Information

Eliza Schreibman

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 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 doxed.

CONTACT

Eliza Schreibman
Tufts University, School of Engineering
Eliza.schreibman@tufts.edu

INTRODUCTION

Doxing (or 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.
The four cornerstones to doxing are:

- Mob mentality/hive mind of the attackers
- Information is usually publicly available
- Attackers connect information and build a detailed profile[1]
- Attacks are motivated by wanting to harm to the victim (with no benefits or gains to the attackers)[2]

These factors all combine to make doxing an extremely powerful tool that can be wielded by anyone.

ATTACKS

Attack principles:

- Gather as much information as possible, including information on friends, family, and co-workers
- Looking for full name, age, picture, usernames, social media accounts, email, phone number, IP address, passwords, credit cards, bank accounts, social security number, medical history, home/work address, etc.
- Connect this information to better understand the target
- Use these to better find sensitive information such as
- Intimidate, harass, and shame the target

Common attack methods[3]

- Basic search engines (e.g. Google, Bing, Yahoo)
- Person information search engines (e.g. Spokeo, Whitepages, Pipland)
- IP address can be found via email header, lookup sites (iplocation), or UNIX commands like ping, lookup, traceroute, and finger[4]
- Cracking passwords tools such as John the Ripper or Hashcat
- Acquiring master password to a password manager such as site such as Last Pass or 1Password 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.).
- Home address can be found on sites like whois, 411 and whitepages..

DEFENSE

Defense principles:

- There is no full-proof way to prevent doxing or remove all information
- Focus on minimizing public sensitive information and secure private information
- Doxing is never the victims fault and there is no one right way to react

Prevention[5]

- Search yourself like a doxer would and see what information you can find
- Remove yourself from 3rd party information seller lists
- Increase privacy settings on social media accounts
- Use two-factor authentication when possible
- Use a good password manager with a strong master password
- Never open suspicious links and be wary of unsecure wireless networks

Defense and Damage Control[6]

- If your physical safety is in danger, call the police
- Freeze compromised accounts, credit cards, emails
- “Watch the watchers” aka monitor the doxers to see what information they have obtained and what they are attempting to do with it

WHY SHOULD WE CARE?

While I am not here to claim that doxing is inherently evil, it is undeniable that 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, Brianna Wu, and Anita Sarkeesian. 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. What’s even scarier 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 irony that legal repercussions are all but non-existent for attackers, despite the fact that all the threats and information posts are publically available. 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.

CONCLUSIONS

Doxing is the fast food of privacy ruining: its quick, easy, cheap, and popular. It requires little skill or thought on the attacker’s part, yet the power it gives is enormous. Additionally, many people love or require the Internet for their school, work, or own enjoyment. Doxers often have the added strength of their anonymity, mob mentality, and lack of legal repercussions. This is, admittedly, a bleak prospect, a national issue that needs to be taken more seriously by technology companies (such as social media sites, internet providers, and 3rd party information sellers) and legal groups alike. In the meantime, we have the power to not only speak up about the issue but also to protect our loved ones and ourselves. We cannot underestimate the power of awareness, since many people have *no idea* how vulnerable they are. Once we know what data is out there, we can prune our public Internet presence and better secure private information. Additionally, we can all be more sensitive to how traumatizing doxing (and any form of harassment) can be and stop blaming people for having personal information on the Internet. There is no sure-fire way to prevent doxing or any other privacy invasion—short of becoming literally invisible—but that doesn’t mean we are powerless. The Internet is a double-edged sword, but if we wield it consciously and carefully, we might not get cut.

FUTURE WORK

I would love to further this paper in the future by

- Explore the vulnerabilities and prevention tools for technologies besides computers (e.g. smart phones, wearables, etc.)
- Interview a victim of doxing
- Attempt a safe and controlled doxing experiment to see how these defenses hold up in real life

REFERENCES

1. Cox, Joseph. "I Was Taught to Dox by a Master." *The Daily Dot*. 6 Jan. 2015. Web. 14 Dec. 2015.
2. Mattise, Nathan. "Anti-doxing Strategy—or, How to Avoid 50 Qurans and $287 of Chick-Fil-A." 15 Mar. 2015. Web. 14 Dec. 2015.
3. "How to Dox Anyone." *Ctrlaltnarwhal*. 21 Oct. 2012. Web. 14 Dec. 2015.
4. "Preventing Doxing." *Crash Override Network* -. 17 Jan. 2015. Web. 15 Dec. 2015.
5. 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.
6. "So You’ve Been Doxed: A Guide to Best Practices." *Crash Override Network*. 21 Mar. 2015. Web. 15 Dec. 2015.