

This is part of training material released by The New York Times. For more information, please read [this article on NYT Open](#) and see [this resource guide](#). If you wish to make changes to this doc, please make a copy using the dropdown menu under “File” above.

Doxxing Curriculum Guide

Guide for workshop facilitators

Overview

Class Subject: Accessing your online footprint

Length of Lesson: 1.5 hours long

Level: Beginner

Doxxing is a low-level tactic used by malicious actors online to acquire and expose the personal information of public figures, including journalists. This information is commonly pulled from a mix of public records, social media accounts and publications.

In this 90-minute workshop, students will learn how to find and understand the extent of their online footprint, secure their accounts and take steps to limit their data exposure online. They will also gain hands-on experience with open source tools and strategies commonly leveraged by bad actors in these types of attacks to take control of your identity online.

What will participants learn?

Participants will learn how to utilize the techniques and tools attackers use to gather personal information on a target to understand the extent of their footprint online. Once they have assessed their footprint, they will learn how to reduce the amount of online data that can be used to target them with doxxing attacks and other online threats.

What materials will participants need?

A computer and an internet connection.

Post-workshop recommendations

- Create a chat room, where students can answer questions after the workshop.
- Share a link or attachment of the *Doxxing Yourself Online Guide* included in the class.

- Set up office hours, or another informal meeting, where attendees have the option to swing by during a designated time to continue working through removing their data

Outline of workshop

Introduction

The first section of this workshop should introduce participants to the concept of doxxing and how it is used the target at-risk groups, such as journalists.

Section slides:

- What is doxxing?
 - Dox: Search for and publish private or identifying information about (a particular individual) on the internet, typically with malicious intent.
 - Hackers and online vigilantes routinely dox both public and private figures.
- Doxxing as a tactic
 - Doxxing is a historically low level, yet effective tactic used by many different types of actors on the internet, including cybercriminals, hacktivists, trolls, and hacking groups.
 - Doxxing is now a normal tactic used to target journalists
- Why do people dox?
 - Exposing personal data for other people to target
 - Demonstrating that you can acquire sensitive information about someone
 - Exposing sensitive information about an individual for the purpose of proving a point
- What info do doxxers look for?
 - Phone number(s)
 - Current home address(es)
 - Past home address(es)
 - Email address(es)
 - Hometown
 - Names of family members
 - Birth date
 - Location of work
 - Vehicle information
 - Embarrassing info/pictures
 - Political/ religious affiliations
- Let's dox ourselves before we get doxxed...
 - By helping people identify and decrease their online footprint to reduce opportunity for doxxing or other malicious targeting.
 - We are not recommending that you erase your online footprint.

Search Engines

In this section, overview how search engines are used to locate basic information that can be used as pivot points. Teach students how to leverage search operators and different search engines to find more specific results about themselves.

Section slides:

- Introduction to search engines
 - Search engines are often a starting point for doxxers
 - Used as initial reconnaissance to gather basic info about an individual
 - Data found is often used as pivot points to find other data (This is covered in the following 2 sections)
- Common search operators (choose the operators that you think will be of most value to the participants)
 - “Quotes”
 - AND/OR
 - Site:
 - Filetype:
 - -Hyphen
 - *Asterisk
- Case Study
 - *Use the case study section to provide an example of search operators in action. Using yourself as an example can resonate with your students.*
- Exercise (10 minutes)
 - Using Google’s search operators, search yourself and see what type of information is available in the first couple pages of search results.
 - Example searches can be found in the guide.

Public Record/Data Brokers

In this section, students will learn how data broker websites work about how to safely engage with them with the goal of reducing their information.

Section slides:

- Introduction to public record and data broker websites
 - Leverage search engines to find specific sites that your information is listed
 - Can identify relationships, addresses, email addresses, phone numbers, & more
 - Often used by doxxers to correlate data & confirm targets
- Data broker websites
 - There are many public record sites that make it difficult to remove your data
 - They are often poorly maintained and difficult to search.

- They can be used by other data broker websites to aggregate data in easily searchable ways.
- These sites are sketchy
 - They collect your data and, often times, sell it!
 - Often they request sensitive personal data to remove yourself from their database
 - Some claim to remove your profile, but don't actually do it.
 - Some may sell your data if you attempt to opt out.
- Opting out
 - Most of these sites have opt out procedures that you can follow to remove your information from the sites.
 - Do:
 - Set up a virtual phone number, like Google Voice or Sudo.
 - Create a separate, "burner" email address.
 - Don't:
 - Don't provide any new information to these sites.
 - Use an old mailing address for verification.
 - Don't EVER provide a copy of any documents, such as driver's license or passport.
- Case study
 - *Walk through searching a couple common data broker websites. If you are using someone else's information, be sure to redact anything that is sensitive,*
- Yes, your data may show up again
 - These sites are pulling data from public records and open source, so if you move, get married, or make another life change, it's possible your data may repopulate on these sites.
 - Solution: Spring cleaning! Make this a once-a-year process to keep your online footprint at bay
- A note for participants based outside of the US.
 - The list of sites we share in the tipsheet primarily query individuals who currently live, or have lived at one point, in the United States. There are significantly fewer data broker sites that query data for individuals in different countries.
- Mitigation
 - Remove your profiles from data broker websites.
 - Spring cleaning!
 - Make this a yearly task.
 - Share this list with your friends and family.
- Exercise: 10-15 minutes
 - Go through the list of data broker sites in your guide and see if you can find your own profiles.
 - Consider following the opt-out steps detailed in the guide to remove your data.

Social Media

In this section we focus on the most commonly used social media apps in our newsroom. Feel free to adjust this section based on your audience.

Section slides:

- Introduction to social media
 - Doxxers often use data gathered from search engines & data broker sites.
 - Social media is used to gather specifics about relationships, hobbies, travels.
 - Information found here is also used by malicious individuals and groups for social engineering, phishing & password/security question guessing.
- What are doxxers looking for?
 - Job & school history
 - Favorite music, movies, & food
 - Your friends & family
 - People who endorse your skills
 - Vacations you've taken
 - Places you've lived
 - Your geolocation
 - Your emotional state
 - What you are doing right now
- Facebook
 - Searching in Facebook
 - Facebook's internal search provides a limited set of options when it comes to searching accounts.
 - To get an accurate view of what is public, partner with someone who is not friends with you on Facebook when searching this platform.
 - Case study
 - *Provide example of using Facebook search to find information on a profile. Be sure to redact any sensitive information.*
 - Locking down your Facebook account
 - Hide your friends list from public view.
 - Edit who can look up your profile using your email or phone number
 - Disallow search engines from linking to your profile
 - Review how others can interact and post to your timeline
 - Review who can tag your account in posts and pictures
- Twitter
 - Searching in Twitter
 - Twitter's [advanced search](#) allows you to get specific when searching for tweets by location, mentions, and date range.
 - Old tweets tend to be dug up in doxxing attempts, this is a good area to audit.

- Lock down your Twitter account
 - Edit who can look up your profile using your email or phone number
 - Disable location information on Tweets
 - Disable photo tagging
 - Audit old tweets
 - Search for keywords of sensitive information like your birthday or children's names and delete tweets
- LinkedIn
 - Searching LinkedIn
 - Some social media sites don't have great search tool like LinkedIn.
 - In this case, you can leverage Google to search site specific information.
 - Example search operator
 - Site:linkedin.com "Investigative Reporter at COMPANY NAME"
 - Lock down your LinkedIn
 - Edit who can look up your profile using your email or phone number
 - Disable the visibility of your profile to non-LinkedIn users
 - Update the visibility of your email address to first degree connections
 - Limit who can see your connections
- Exercise (10 minutes)
 - Using the Doxxing Guide and the Social Media Security & Privacy Checklists, audit your social media accounts for sensitive information. Start configuring the security and privacy settings on your social media accounts.

Closing

Students may feel overwhelmed at this point, so I recommend ending the workshop with some tips on how to go about cleaning up the rest of their footprint.

Section slides:

- Break it down: we've formatted the tipsheet to help you tackle this section by section.
- The more the merrier: make this a partner or group activity! Friday nights were meant for drinking wine and cleaning up your online footprint.
- Your contact information (*For follow-up questions*)