NYC Digital Safety
Privacy & Security

Doxing

Facilitation Guide

Gently lead a conversation with learners about the risks and issues posed by doxing. Help them know what to do if they fall victim to doxing.

Overview

This module introduces learners to doxing and exploring what doxing is, why it happens, and what to do in the event of a doxing attack. Doxing is a serious form of online harassment. This module will equip learners with knowledge and skills to help them better understand how and why doxing happens, what actions they can take to better avoid doxing, and what to do if they become the victim of a doxing attack.

For more information, be sure to watch Series 2 of training videos on NYC Digital Safety.

Outcomes

By the end of this module, participants will be able to:

- Define doxing
- Discuss the causes and effects of doxing
- Identify and use different approaches for both avoiding doxing and dealing with a doxing attack that has occurred

Format + Time Frame

This module provides an information overview of doxing and examines what doxing is, how and why doxing happens, and what the effects doxing can have on victims. This module will also include guidance on both how to lessen the risk of becoming the target of a doxing attack and what to do in the event of a doxing attack.

This module will take approximately 40 minutes to complete. It can be extended to 60 minutes with optional discussions and activities.

Materials

- Slide deck
- Facilitation guide
- Handout

Lesson Plan

Activity	Materials	Time Needed
Introduction and welcome Greet learners and review the plan for this module.	Slides 1 through 3	2 minutes
Define doxing Provide a working definition of doxing. See if anyone has any questions or anything to add.	Slide 4	3 minutes
Discussion: Your experiences with doxing Ask your learners to discuss and share what they know about doxing and see if any of them have any examples or incidents they've heard about to share.	Slide 5	5 minutes
What doxing is and how it happens Share basic concepts around doxing and why it occurs.	Slides 6 through 11	10 minutes

Pause to see if your learners have anything else to add to these lists.		
Discussion: Cyberbullying [optional] Ask learners to share examples, experiences with, or thoughts on cyberbullying.	Slide 12	10 minutes
What to do during a doxing incident Review steps for what to do if you've been doxed.	Slides 13 through 16	5 minutes
Strategies to use to avoid doxing Share best practices for avoiding an incident in the future.	Slides 17 through 20	5 minutes
Activity: How to avoid doxing [optional] Put learners into small groups. Have them discuss and brainstorm ways to avoid doxing.	Slide 21	10 minutes
Doxing and online participation Emphasize that doxing is often used as a tool to initiate and threaten people. Encourage learners to protect their online security and to take steps to protect themselves from doxing.	Slide 22	5 minutes
Wrap up, final tips, and final questions Review the closing thoughts and share the suggested resources. See if anyone has any final questions.	Slide 23 through 27	5 minutes

Considerations

Doxing is an alarming phenomenon that is increasingly impacting individuals online. Doxing is a serious form of harassment and a doxing attack can have serious repercussions for the victim. Given the serious and even frightening nature of this topic, consider leaving space in your workshop for discussion and questions so that learners have the time and space to process and unpack the issues you are raising in the module.

You might also consider having some sort of community participation guidelines before starting the module, given the sometimes sensitive nature of this topic (see a sample of this in the slide deck). Additionally, consider making yourself available after the module for one-on-one conversation in case someone has an issue or question that they don't feel comfortable raising in front of an entire group. Doxing has been used to silence, harass, or target minority groups online, including women, people of color, LGBTQIA individuals, and others. It is important to keep in mind the ways in which people in your audience might have experienced things like cyberbullying or online harassment before.

For this module, you might consider spending some extra time reviewing the video and recommended resources included there to learn more about this complicated topic.

Options and Variations

This module delves into a lot of complex and difficult issues, and stands well on its own. If you are interested in exploring connections to other modules, you might consider offering this module as part of a longer series of workshops, where you can have the time and space to fully unpack and explore each module. Some options for pairing could include modules on Data Generation and Data Minimization, Social Media Accounts, and online privacy more generally.

This content is fairly complex but, if you are short on time, you could still share the information here at places like service points via the guided handout. However, given the nature of this topic, you might consider strongly encouraging someone to return for a workshop or come back with questions.

Assessment

The following are some suggested assessment questions that you can use and adapt for your own purposes. These questions can help you assess various things, including knowledge retention, personal views and preferences, and concept application.

You might consider asking these as a pre or post test, or you can have learners answer these as part of an exit survey or a follow-up survey. Keep reading for suggested questions and an answer key with further details and explanations.

Questions for Participants

What is doxing?

A. It's a type of phishing scheme
B. A scam that tricks you into sending personal documents to someone
C. A hack involving Google Docs
D. A form of online harassment where the victim has personal details hacked and publicized online

Who can be the target of a doxing attack?

A. Famous celebrities
B. Online activists
C. Anyone and everyone

What can you do if you are doxed?

A. Report it to law enforcement
B. Report it to platforms where the information was publicized
C. Increase your digital security - for example by changing passwords
D. None of the above
E. All of the above

How can you avoid being doxed?

A. Manage your social media privacy settings
B. Be cautious about revealing personal details online
C. Use different usernames on different platforms
D. All of the above

Answer Key

What is doxing?

Answer: D, A form of online harassment where the victim has personal details hacked and published online

Doxing is a serious form of online harassment where someone publicizes your personal information on the internet. It can lead to harassment campaigns, privacy breaches, and other issues for victims.

Who can be the target of a doxing attack?

Answer: C, anyone and everyone

Increasingly, anyone can become the victim of doxing. It used to happen more to celebrities or well-known individuals, but now anyone can be doxed.

What can you do if you are doxed?

Answer: E, all of the above

If you are doxed, you should report it and also take steps to tighten up your digital security, since doxing attacks expose your information and can lead to hacks and other issues.

How can you avoid being doxed?

Answer: D, all of the above

Managing your privacy settings and digital security, and practicing data minimization can all be ways to help you avoid being doxed.

Connections to Other Modules

This module connects to many other modules. The following suggestions provide opportunities for exploration, connection, and potential programming. However, feel free to explore and make connections between other modules not listed here as well!

1.1 Data Generation

1.2 Data Minimization
1.2 Password Hygiene

1.3 Data Breaches
1.3 Social Media Account Hacks

2.2 Social Media Settings

These and other modules can be found at this project's website, nycdigitalsafety.org.

About This Project

These materials were released in October 2022 as part of NYC Digital Safety: Privacy & Security.

NYC Digital Safety: Privacy & Security is a partnership between New York City's three library systems — Brooklyn Public Library, The New York Public Library, and Queens Library — and METRO Library Council. With support from the New York City Office of Technology and Innovation, this project ensures that NYC residents can rely on public libraries for their questions about internet privacy and security.

Visit nycdigitalsafety.org for more information.