NYC Digital Safety
Privacy & Security

Browser Extensions

Facilitation Guide

Provide learners with best practices for managing their browser extensions.

Overview

This module introduces to learners to best practices for managing their browser history and keeping their browsing activity private and secure.

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

Outcomes

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

- Define and describe browsing extensions
- Understand how browser extensions work
- Discuss the pros and cons of selecting and using browser extensions

Format + Time Frame

This module provides an information overview of browsing history, including what it is and the pros and cons of deleting browsing history, and a how-to guide for ways to manage browsing history.

This module will take approximately 30 minutes to complete. It can be extended to 45 minutes with an optional activity. You can combine this module with others for a longer learning experience.

NYC Digital Safety
Privacy & Security

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 and 2	2 minutes
Defining browser extensions Provide a brief definition of browser extensions and see if anyone has any clarifying questions.	Slide 3	3 minutes
What browser extensions can do Share examples of what browser extensions can do. Ask learners what they would add to this list.	Slide 4	5 minutes
Risks associated with browser extensions Share with learners some of the risks inherent with browser extensions, including the amount of information they can provide to developers. See if anyone has any questions.	Slide 5 and 6	5 minutes

Activity: Ensure your current browser extensions are secure [optional] Give your learners the guided handout. Invite learners to list the browsers they currently use. (Note: learners may need to do this from memory if they don't have access to a personal device. You may consider reviewing this activity and sending it home with learners to practice on their own.) Learners can then research some of their extensions to determine the level of safety.	Slide 7, handout	15 minutes
Managing your browser extensions Share a list of best practices learners for using browser extensions.	Slide 8	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.	Slides 9 through 12	5 minutes

Considerations

While browsing history can pose digital security risks and concerns, it can also be beneficial to have. Spend some time discussing both the benefits and the drawbacks of maintaining browser history versus deleting browser history. You might frame managing, and deleting, browser history as an aspect of an overall digital security maintenance schedule.

Options and Variations

This module pairs well with other modules on managing browsers and online security, particularly the modules on Private Browsing and on Cookies.

You might consider leaving time and space for learners to go through the process of clearing their browsing history and familiarizing themselves with the available browser history settings on their web browser of choice. This can be a way to provide a more extended, hands-on workshop experience.If you have less time, you can equip learners with the guided handout so that they can manage their browser history on their own.

You can also provide this information and content to patrons via a service point by sharing the guided handout with them.

Assessment

Questions

Fill in the blank: “Browser extensions are often created by _____, who may or may not be legitimate. A browser extension from a nefarious source could steal your password, sell your data to advertisers, or redirect you to sites that contain malware.”

True or false: Browser extensions can update automatically, which means they could be hijacked and start collecting your data without you realizing anything is wrong.

A. True
B. False
C. Unsure

Which of the following is NOT a recommendation for safely installing and using browser extensions?

A. Read reviews of the browser extension
B. Look for information on who created the browser extension

C. Install the extension first and look into it later
D. Make sure you understand how the extension works

Answer Key

Fill in the blank: "Browser extensions are often created by _____, who may or may not be legitimate. A browser extension from a nefarious source could steal your password, sell your data to advertisers, or redirect you to sites that contain malware."

Answer: Third-parties

This is why it is important to vet browser extensions before installing them, since some third-party developers might not be legitimate.

True or false: Browser extensions can update automatically, which means they could be hijacked and start collecting your data without you realizing anything is wrong.

Answer: A, True

Make sure you pay attention to your apps. browser extensions, and other things that update automatically since these things can be hijacked without you realizing it.

Which of the following is NOT a recommendation for safely installing and using browser extensions?

Answer: C. Install the extension first and look into it later

Unsafe apps and extensions are a common way for hackers and scammers to deliver malware to a device, so it is never a good idea to install something without first checking out what it is and ensuring it is safe to use.

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!

2.1 Cookies

2.1 Targeted Advertising

2.2 Browser History
2.2 Private Browsing
2.2 Ad 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.