NYC Digital Safety

Privacy & Security

Dealing With Malware and Viruses

Facilitation Guide

Introduce learners to best practices for identifying, avoiding, and dealing with malware and various kinds of viruses.

Overview

This lesson introduces to learners to best practices for avoiding and preventing malware and viruses from getting onto devices, and dealing with malware and viruses that might already be on a device.

For more information, be sure to watch Series 4 training videos from NYC Digital Safety.

Outcomes

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

- Distinguish between malware and viruses
- Describe the ways in which malware and viruses can infect a device
- Identify approaches for preventing and handling malware and viruses that are on a device

Format + Time Frame

This lesson provides an information overview of malware and viruses, including their differences, and examines approaches for dealing with malware and viruses that are on devices.

This lesson will take approximately 50 minutes to complete. You can extend this lesson by giving attendees time to go through the guided handout during the workshop, or you can combine this lesson with others for a longer learning experience.

Materials

- Slide deck
- Facilitation guide
- Handouts
    - Dealing With Malware
    - Checking Credit Reports

Lesson Plan

Activity	Materials	Time Needed
Introduction and welcome Greet learners and review the plan for this lesson	Slides 1 and 2	2 minutes
Defining malware and viruses Review these definitions and pause here for any questions. Make sure everyone is clear on the distinctions between these two.	Slide 3	5 minutes
Discussion: Examples of viruses Ask your learners to share examples of viruses they have seen or heard about, and feel free to contribute your own examples here as well.	Slide 4	7 minutes
Malware and viruses	Slides 5 through 7	10 minutes

Review the examples and types listed on these slides and pause to see if anyone has any other examples to share or experiences with any of the things listed.		
The signs of a malware infection Review the different signs of malware and viruses listed here and pause to see if anyone has experienced any of these things before during a malware or virus infection. If you have a personal example that you feel comfortable sharing, feel free to include it here.	Slide 8	10 minutes
Ways to deal with a malware or virus infection Review the list of strategies here and see if anyone has any questions or needs any clarification about the steps listed.	Slides 9 through 12	10 minutes
Wrap up, final tips, and final questions Review the final suggestions and introduce the resources listed. If you have extra time, consider giving your learners longer to explore the links listed in the resources. See if there are any final questions.	Slides 13 through 16	5 minutes

Considerations

While most people have heard of malware and viruses, they might not be entirely clear on the distinctions between the two. Be sure to spend some time going over the definitions of these terms and ensuring that your learners are clear about the terms introduced in this lesson.

While this lesson provides some examples of different types of malware and viruses, you might also consider bringing in some examples from the news, or from your experiences, and encouraging learners to share examples that they have heard of as well.

Options and Variations

This lesson can be seen as an extension to the other lessons on malware, including the main Malware lesson, the Ransomware lesson, and a lesson on Managing a Malware Attack. The main Malware lesson touches upon content included in this lesson. You could merge the two together, or use this as a shorter, more focused lesson that can support the broader Malware lesson.

It is strongly suggested that you consider either combining the malware lessons or offering these lessons as part of a series on malware. Note that the malware lessons share a master handout on various aspects of malware (see Lesson 3.2 Malware) that can be used as a resource for any or all of the malware lessons.

You can also provide this information and content to patrons via a service point by sharing the guided malware handout with them, though you might consider making sure you combine this handout with other handouts on malware.

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.

Note that for additional, related assessment questions you should use the ones included in the 3.2 Malware Lesson.

Questions for Participants

What is a virus?

A. A type of malware
B. A computer program that infects a device and replicates itself via code
C. Software that can corrupt computer data and software
D. All of the above

Which of the following are examples of computer viruses?

A. Browser Hijacker
B. Spyware
C. Ransomware
D. A Computer worm

True or false: The methods used to avoid and handle malware can be used with computer viruses

A. True
B. False
C. Unsure

Answer Key

What is a virus?

Answer: D, All of the above

Viruses are forms of malware that replicate themselves on a computer.

Which of the following are examples of computer viruses?

Answer: A, Browser Hijacker

A browser hijacker is a type of computer virus that can infect your device and change your browser settings. The other examples here are all forms of malware, just a virus is a form of malware.

True or false: The methods used to avoid and handle malware can be used with computer viruses

Answer: A, True

True. The approaches used to avoid and deal with malware can apply to computer viruses as well

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 Phishing Schemes

1.3 Data Breaches
1.3 Social Media Account Hacks

2.2 Browser Extensions

3.2 Malware
3.2 Pitfalls on Apps and Websites

4.1 Avoiding Social Engineering
4.1 Ransomware

4.2 Managing a Malware Attack

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.