Managing a Malware Attack

Facilitation Guide

Introduce learners to best practices for successfully managing and navigating a malware attack.

Overview

This lesson introduces to learners to best practices navigating and managing a malware attack, including techniques to use and approaches to take during and after an attack.

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

Outcomes

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

- Identify different kinds of malware
- Describe the ways in which malware attacks work
- Identify approaches for managing a malware attack

Format + Time Frame

This lesson provides an overview of different kinds of malware and explains the best practices and strategies to use for managing a malware attack and dealing with the aftermath of a malware attack.

This lesson will take approximately 45 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
- 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 malware Review this definition of malware and note that some forms of malware are more aggressive than others.	Slide 3	5 minutes
Discussion: Malware examples and effects Ask participants what malware can do, and see what examples or ideas they have to share. Consider getting a discussion going by sharing a personal or real-world example of a malware attack.	Slide 4	7 minutes
More aggressive types of malware 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.	Slides 5 and 6	5 minutes

The signs of a malware infection Review the different signs of malware listed here and pause to see if anyone has experienced any of these things during a malware attack in the past. If you have a personal example that you feel comfortable sharing, feel free to include it here.	Slide 7	5 minutes
What to do during and after a malware attack Review the list of strategies here and see if anyone has any questions or needs any clarification about the steps listed.	Slides 8 and 9	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 participants longer to explore the links listed in the resources. See if there are any final questions.	Slides 10 through 13	5 minutes

Considerations

While malware ecompasses many different kinds of malicious software, this particular lesson delves into malware that engages in more overt and disruptive attacks, such as ransomware or worms. While this lesson provides some examples of different types of malware, 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 Dealing with Malware and Viruses. The main Malware lesson and the Ransomware lesson both touch upon content included in this lesson. You could merge these lessons together, or use this as a shorter, more focused lesson that can support the broader Malware lesson and the more focused Ransomware 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, namely the ransomware handout.

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 or the 4.1 Ransomware Lesson.

Questions for Participants

Which of the following are types of malware? Select all that apply:

A. A virus
B. A computer worm
C. Ransomware
D. Spyware
E. All of the above

True or false: Malware cannot infect Apple devices.

A. True
B. False
C. Unsure

True or false: For a severe malware infection, you might need to reinstall your operating system.

A. True
B. False
C. Unsure

Answer Key

Which of the following are types of malware? Select all that apply

Answer: E, all of the above

Malware is an umbrella term that includes viruses, spyware, worms, and other malicious softwares.

True or false: Malware cannot infect Apple devices

Answer: B, False

False. While Apple devices historically had less issues with viruses and malware, they are still, and are now increasingly, vulnerable to them.

True or false: For a severe malware infection, you might need to reinstall your operating system

Answer: A, True

True. Severe infections could mean that you need to reinstall your operating system. Make sure to use directions from your device manufacturer on how to do this correctly and safely.

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 Dealing with Malware and Viruses

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.