NYC Digital Safety
Privacy & Security

Ransomware

Facilitation Guide

Alert learners to the risks posed by ransomware, and help learners know what to do if they become the victims of a ransomware attack.

Overview

This module introduces to learners to the risks posed by ransomware and equips them with the knowledge and skills to know how to manage a potential ransomware attack and to avoid ransomware in the future.

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:

- Define ransomware
- Describe how ransomware works
- Identify approaches for handling and avoiding ransomware attacks

Format + Time Frame

This module provides an information overview of ransomware and explains what actions to take in the event of a ransomware attack and how to avoid possible ransomware attacks in the future.

This module will take approximately 50 minutes to complete. This module tackles a fairly complex topic. But you can combine this module with other, related modules for a more extensive learning experience.

Materials

- Slide deck
- Facilitation guide

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 ransomware Pass out the handout now, or at any point in the lesson. Provide a brief definition of ransomware and pause to see if anyone has any questions or anything to add to the definition.	Slide 3, handout	3 minutes
Discussion: Examples of ransomware Put participants into small groups. Have them brainstorm about examples of ransomware they might have heard about or even experienced before. Have them report back on what they discussed.	Slide 4	5 minutes
Ransomware attacks Review what happens during a ransomware attack, including the infection and attack phase.	Slides 5 through 7	5 minutes

Review the information on who is targeted by ransomware. Pause to see if there are any questions.		
Ways to manage a ransomware attack Review the steps and suggestions for ways to manage a ransomware attack and to avoid or prevent such attacks. See if anyone has any other suggestions to add.	Slides 8 and 9	10 minutes
Activity: Avoiding ransomware Have your learners get into small groups. Have them review and discuss best practices for avoiding scams and malware, as a way to avoid ransomware.	Slide 10	15 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 11 through 13	10 minutes

Considerations

Ransomware is a tricky and alarming topic to cover. While ransomware attacks often target businesses or organizations, individuals can also be targeted by these attacks. And learners might have gone through a ransomware attack at their own workplace. Given the complex nature of this topic, consider leaving extra time for questions and discussions. Additionally, you might want to emphasize empowering tips and strategies that learners can use to deal with ransomware, since ransomware attacks are designed to make people feel helpless or vulnerable.

Since most of the tips for avoiding ransomware connect to modules on malware, phishing schemes, text and email spam, etc., you might consider offering this workshop after offering those. Or you could combine this workshop with another workshop, or a series, on avoiding schemes and malware.

Options and Variations

This module delves into a lot of complex 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. Or, if you have extra time, you could combine this module with other related ones for a longer workshop experience. Some options for pairing could include modules on Malware, Data Breaches, and Social Media Account Hacks.

There is a good bit of content to cover here but, if you are short on time, you could still share the information at places like service point via guided handouts, like the one on Malware. 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 ransomware?

A. A type of computer virus
B. A sort of targeted ad
C. A type of malware that prevents a user from accessing their system

D. A type of phishing scheme

Who can be targeted by ransomware? Select all that apply.

A. Large corporations
B. Small businesses
C. Individuals
D. Government agencies
E. All of the above

What is something you should not do to keep yourself safe from ransomware?

A. Secure your accounts and passwords
B. Use private browsing
C. Be informed about how to avoid phishing schemes and scams
D. Be cautious with clicking unknown links or opening files from unknown sources

Have you or your workplace ever had to deal with ransomware?

A. Yes
B. No
C. Unsure

Answer Key

What is ransomware?

Answer: C, A type of malware that prevents a user from accessing their system

Ransomware is a type of malware that effectively holds your device hostage for ransom. Ransomware locks people out of their systems and files. While it is similar to a virus, ransomware is not technically considered a computer virus. Rather, it's part of the broader malware family.

Who can be targeted by ransomware? Select all that apply.

Answer: E, all of the above

Ransomware mostly targets small and medium businesses but anyone and everyone can be targets and ransomware is growing increasingly widespread.

What is something you should not do to keep yourself safe from ransomware?

Answer: B, private browsing

You can avoid ransomware by using good data security practices and by being aware of and alert to things like schemes, which are often how people get exposed to ransomware. Private browsing doesn't do all that much to help in this situation.

Have you or your workplace ever had to deal with ransomware?

Answer: No correct answer

You can use this question as a pre-test question to generate discussion or as a follow-up question to learn more about your audience.

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

3.2 Pitfalls on Apps and Websites
3.2 Malware
3.2 Identifying Email and Text Spam

4.1 Social Engineering

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.