Malware Facilitation Guide

Share best practices for identifying, avoiding, and dealing with malware.

Overview

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

For more information, be sure to watch Series 3 training videos from NYC Digital Safety.

Outcomes

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

- Define malware
- Describe the ways in which malware can infect a device
- Identify approaches for preventing and handling malware attacks

Format + Time Frame

This module provides an information overview of malware and explains what malware is, how it works, and ways to avoid and handle malware on different kinds of devices, including phones and computers.

This module will take approximately 45 to 50 minutes to complete. You can extend this module by giving attendees time to go through the guided handout during the workshop, or you can combine this module with others for a longer learning experience.
## Materials
- Slide deck
- Facilitation guide
- Handout

## Lesson Plan

<table>
<thead>
<tr>
<th>Activity</th>
<th>Materials</th>
<th>Time Needed</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Introduction and welcome</strong></td>
<td>Slides 1 and 2</td>
<td>2 minutes</td>
</tr>
<tr>
<td>Greet learners and review the plan for this module.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Definition malware                 | Slide 3         | 2 minutes   |
| Provide the handout to learners at any point during this lesson. |                 |             |
| Provide a brief definition of malware and pause to see if anyone has any questions or anything to add. |                 |             |

| Discussion: Your experiences with malware | Slide 4 | 7 minutes |
| Break participants into pairs or small groups and have them discuss their experiences with malware. |                 |             |
| Have the groups share what they discussed with the entire group. |                 |             |

| How malware works                   | Slides 5 through 9 | 10 minutes |
| Review different types of malware, how malware infects devices, and how to identify malware. |                 |             |
Briefly pause after each slide to see if there are any questions or if anyone has something to add.

<table>
<thead>
<tr>
<th>Ways to deal with malware</th>
<th>Slides 10 and 11</th>
<th>10 minutes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review the different strategies listed here and see if anyone has any other strategies to add or if they need something clarified.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ways to avoid malware</th>
<th>Slides 12 and 13</th>
<th>7 minutes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review the different approaches listed on the slides and see if anyone has anything else to add to the list.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Wrap up, final tips, and final questions</th>
<th>Slides 14 through 17</th>
<th>7 minutes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review the closing thoughts and share the suggested resources. See if anyone has any final questions.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Considerations**

Malware is something most people have heard about, or have had direct experiences with in the past. This topic can generate a good bit of conversation and discussion since it is so familiar to so many, so you might consider leaving some additional time for questions, discussion, and just general conversation around this topic.

**Options and Variations**

This module pairs well with other modules about online security, including phishing schemes and scams and modules about actions to take in the event of a hack. You could consider either combining modules or running a whole workshop series on securing devices and dealing with scams, schemes, hackers, and malware.
While the handout for this module contains tips and advice for both dealing with malware that might already be on a device, and preventing malware from getting there in the first place, the suggestions are not necessarily things that would work well in a workshop setting. For example, you might not want to spend lots of time having attendees download antivirus software during a workshop. If you'd like to have a more extended, hands-on experience, consider leaving time for discussion and encouraging attendees to develop an action plan of steps they can take after the workshop is over.

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

**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 malware?

A. A type of targeted ad  
B. A form of spam email  
C. A software program deliberately designed to disrupt or gain unauthorized access to a computing device  
D. A phishing schemes that tries to fool someone into giving away their password

Which of the following are types of malware?

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

How can you get rid of malware? Select all that apply.  
A. Restart your computer  
B. Scan your device using security software  
C. Reinstall your operating system if the malware infection is severe  
D. Update your account security settings

How can you avoid malware? 
A. Don’t click on pop-ups  
B. Avoid opening attachments from unknown or suspicious sources  
C. Be cautious when downloading apps and software  
D. All of the above

Answer Key  
What is malware?  
*Answer: C, A software program deliberately designed to disrupt or gain unauthorized access to a computing device*  
Malware stands for “malicious software” and is a type of software that can infect devices and cause disruptions or steal information. Malware can affect phones, tablets, and computers.

Which of the following are types of malware?  
*Answer: E, All of the above*  
Malware is sort of an umbrella term that covers a range of things like viruses, spyware, and ransomware.
How can you get rid of malware? Select all that apply.

*Answer: B, Scan your device using security software; C, Reinstall your operating system if the malware infection is severe*

Scanning for malware or (in bad cases) reinstalling an operating system are approaches for removing malware. Simply restarting a device or updating security settings won’t get rid of a malware infection.

How can you avoid malware?

*Answer: D, All of the above*

Malware can be avoided by being cautious with what you download, click, or open!

**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 Pitfalls on Apps and Websites

4.1 Social Engineering
4.1 Ransomware

These and other modules can be found at this project’s website, nycdigitalsafety.org.
NYC Digital Safety
Privacy & Security

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.