Phishing Schemes

Facilitation Guide

Introduce learners to phishing schemes with an interactive activity.

Overview

This module will help learners better understand and identify different types of phishing schemes that they might encounter online.

For more information, be sure to watch Series 1 of the NYC Digital Safety Training videos.

Outcomes

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

- Define and discuss phishing schemes
- Identify different types of phishing schemes
- Name the trends and common features that many different phishing schemes share

Format + Time Frame

This module introduces learners to phishing schemes, including what they are, how they work, and how to be alert to potential scams, with an interactive game.

This module will take approximately 50 to 60 minutes to complete. This activity can be paired with other modules, including modules on online security best practices and online account management, for a more varied, and 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 and discussing phishing schemes Provide a definition of phishing schemes and pause to see if anyone has any questions or anything to add. Ask your learners to share what they know about phishing schemes and what examples they've seen or encountered before.	Slide 3 and 4	10 minutes
Phishing schemes Share some common traits of phishing schemes. See if anyone has anything else to add.	Slides 5 through 7	7 minutes
Detecting and avoiding phishing schemes Share some best practices for detecting and avoiding phishing schemes and see if anyone has anything to add to the lists.	Slides 8 and 9	7 minutes
Activity: Exploring phishing schemes Give learners the guided handout.	Slide 10 and handout	20 minutes

First, have them take a quiz on phishing schemes, sponsored by Google and Jigsaw. Next, have them get into small groups and explore examples of phishing schemes, making note of trends and techniques used.		
Wrap up, final tips, and final questions Review the closing thoughts and resources and see if anyone has any final questions.	Slides 11 through 14	5 minutes

Considerations

Be sure everyone is clear on the definition of phishing schemes before starting the game. You use the information in the handout and the talking points here to share information with your patrons.

Spend some time going over the directions of the game before everyone gets started and make sure everyone understands the game.

Depending on the size of your group, you might have people complete this game in small groups or teams, or you can have people do the game individually and then discuss their results with the entire group once they are done.

Options and Variations

This game works well as a stand-alone activity and it can also be paired with other modules around schemes and scams. Alternatively, this game can feature as part of a series of programming dedicated to exploring schemes and scams. While patrons could play this game on their own, this activity would work best as a group activity in a workshop or class.

If you do not have time to run the full game yourself, you can provide information about phishing schemes to your patrons via the 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.

Questions for Participants

What is a phishing scheme?

A. A scam involving counterfeit checks
B. A tactic that convinces you to join a multi-level marketing scheme
C. A scheme where someone distracts you and steals your credit card information
D. A scam that tricks you into revealing or granting access to your personal information

Which of the following are types of phishing schemes? Select all that apply

A. An email from an unknown sender telling you your account is compromised
B. A strange message from the IRS insisting you owe money
C. A message telling you that you won a free vacation
D. A hacker steals your information from a database

What is not a way to avoid falling for a phishing scheme?

A. Be careful with what you click, open, or download
B. Reply to the sender to find out more and determine if they are legitimate
C. Double check the sender of any requests, especially requests for sensitive information
D. Make sure your security settings are up-to-date on your devices

Answer Key

What is a phishing scheme?

Answer: D

Phishing schemes try to trick you into willingly revealing personal information or into performing a task (like opening a file) that enables a hacker to steal your information.

Which of the following are types of phishing schemes? Select all that apply

Answer: A, B, C

Answers A-C are all common types of phishing schemes, where you get a message that prompts you to reveal your personal information. Some of these messages are alarming and try to scare you, while others might tempt you with a bogus "reward." D is an example of a digital security issue known as a data breach.

What is not a way to avoid falling for a phishing scheme?

Answer: B, Reply to the sender to find out more and determine if they are legitimate

Updating security settings and being cautious with emails asking for personal information are good ways to avoid phishing schemes. B is something you should not do! Do not respond to these scams, since that can reveal your information to the scammer, grant them access to your machine, or otherwise compromise your security. You can delete or report scam messages.

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!

3.1 Spoofed Numbers

3.1 Spam Calls

3.1 Handling Spam Calls

3.2 Dealing with Scammers

3.2 Managing SMS Settings

4.1 Social Engineerings
4.1 Avoiding 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.