NYC Digital Safety
Privacy & Security

Identifying Email and Text Spam
Facilitation Guide

Help learners get better at identifying email and text spam messages.

Overview

This module helps learners get better at identifying email and text spam and introduces them to common elements and traits to look for in both email and text spam. This module utilizes an interactive game to help learners better understand how email and text spam operate.

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:

- Describe email and text spam
- Name common aspects and traits of email and text spam
- Identify examples of email and text spam

Format + Time Frame

This module provides an overview of common aspects and traits of email and text spam and features an interactive game where learners can develop and test their knowledge.

This module will take approximately 60 minutes to complete and includes an activity and time for discussion.

NYC Digital Safety
Privacy & Security

Materials

- Presentation slides
- Facilitation guide
- Handouts
  - Identifying Email and Text Spam
  - Dealing With Scammers

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 email and text spam Provide a brief overview of email and text spam and see if anyone has anything else to add.	Slide 3	3 minutes
Discussion Have learners volunteer to share their experiences with email and text spam. You can kick off the conversation by sharing some examples of your own, if you are comfortable doing so.	Slides 4 and 5	5 minutes
Types of spam Provide a brief overview of common traits seen in different kinds of spam. See if anyone has questions or anything else to add.	Slide 6	10 minutes

Activity, Part 1 : Reviewing text and email spam examples	Slide 7, Handout 1	15 minutes
Divide participants into small groups and have them visit the website listed on the handout. This NY DMV site keeps a running and up-to-date list of scams and spam.		
You can either have a pre-selected list for learners to explore or let them explore the site freely.		
Encourage your learners to make note of trends, themes, and identify key components of the examples they examine.		
Activity, art 2 : Personal examples	Slide 7, Handout 1	15 minutes
Have participants remain in their small groups.		
For this next part, encourage participants to pull up their own text messages and email (have them visit their junk folder) and look for further examples of spam.		
Have your learners identify trends, themes, and key components.		
Activity wrap up	Slide 7, Handout 1	10 minutes
Have your learners generate a list of the common trends and themes they noted in their spam examples.		
Have your learners share their lists with the entire group and share any final observations.		

Wrap up, final tips, and final questions	Slides 8 through 10, Handout 2	5 minutes
Review the closing thoughts and share the suggested resources. Give learners Handout 2. See if anyone has any final questions		

Considerations

Email and text spam are unfortunately things we have all experienced, and these sorts of messages are growing increasingly common. You might consider leaving time for discussion and for learners to share their own examples and experiences with these types of spam messages.

This game is designed to help learners gain confidence in skill in identifying email and text spam. While this game provides some examples for learners to examine together, you can definitely consider having learners share examples of spam messages (if they feel comfortable doing so) to generate further discussion around ways to spot these sorts of spam messages.

You might consider sharing handouts and resources from some related modules, including Phishing Schemes, Dealing with Scammers, and Avoiding Social Engineering.

Options and Variations

This game is designed to be done with a group of learners, ideally in person. If you are doing an online workshop, you could adapt this game by having learners get into small groups in breakout rooms and work through the examples together, or you could use a poll or online quiz software to help learners work through the content.

While this game is designed as a group activity, you could still share it with an individual learner and have them work through the material on their own via the guided handout. If a learner is completing the activity and handout on their own, be sure to supply them with an answer key.

Assessment

The following are some suggested assessment questions that you can use and adapt for your own purposes. 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 explanation.

Questions for Participants

Do you feel that you receive a lot of spam over text or email?

    A. Yes, I receive way too much

    B. I receive some but it isn't overwhelming

    C. I don't receive much spam

What is not a sign of a spam message?

    A. A sense of urgency

    B. Grammar or spelling issues

    C. The message contains a coupon

    D. The message has a lot of strange URLs

What is the goal of spam messages?

    A. Just to annoy you

    B. These messages usually contain phishing schemes or malware and are a ways to get your personal information

    C. They're trying to sell you something

    D. To get views and attention

Answer Key

Do you feel that you receive a lot of spam over text or email?

Answer: Opinion question, no correct answer

This question is aimed at getting a sense of the views of your learners and can be used for generating discussion if used a pre-test question.

What is not a sign of a spam message?

> *Answer: C, the message contains a coupon*

> As with phishing schemes, text and email scam often contain a false sense of urgency, spelling errors, and lots of suspicious links for you to click. While some spam messages might try to trick you with a fake coupon, a coupon isn't a definite sign of spam.

What is the goal of spam messages?

> *Answer: B, These messages usually contain phishing schemes or malware and are a ways to get your personal information*

> Spam messages are generally vehicles for malware or phishing schemes, both of which are aimed at getting your personal information.

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 Social Media Account Hacks

3.1 Handling Spam Calls

3.1 Spoofed Numbers

3.1 Identifying Scam Calls

3.2. Identifying Spam

3.2 Dealing with Scammers

3.2 Managing SMS Settings

4.1 Avoiding Social Engineering

NYC Digital Safety
Privacy & Security

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.