# Avoiding Social Engineering

## Facilitation Guide

*Alert learners to the risks posed by social engineering and empower learners to avoid and handle social engineering attacks.*

## Overview

This module introduces to learners to the risks posed by social engineering and equips learners with the knowledge and skills to know how to handle social engineering and to avoid falling for scams and schemes.

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 social engineering
- Describe how social engineering works
- Identify approaches for handling and avoiding social engineering

## Format + Time Frame

This module provides an information overview of social engineering and introduces learners to different approaches that they can use to better recognize and avoid social engineering.

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 if you wish.

## Materials

- Slide deck
- Facilitation guide
- Handout

## Lesson Plan

| Activity | Materials | Time Needed |
|---|---|---|
| **Introduction and welcome**<br>Greet learners and review the plan for this module. | Slides 1 and 2 | 2 minutes |
| **Defining social engineering**<br>Provide a brief definition of social engineering and see if anyone has any questions or anything to add. | Slide 3 | 3 minutes |
| **Discussion: Manipulation techniques**<br>Ask your learners to consider and share manipulation techniques that are commonly used by scammers. Get a crowdsourced list going. | Slide 4 | 5 minutes |
| **How social engineering works**<br>Provide an overview of how social engineering attacks work, including the steps and methods used by scammers.<br>Review the principles of persuasion. Pause to see if learners have noticed any of these before in spam/scam messages they might have received. | Slides 5 through 7 | 10 minutes |

| | | |
|---|---|---|
| Review the ways in which social engineering scams target people.<br>Pause to see if there are any questions. | | |
| **Types of social engineering attacks and common signs**<br>Review some examples of common kinds of social engineering attacks.<br>Pause to see if anyone has questions or anything else to add.<br>Review some of the warning signs of social engineering. | Slides 8 through 12 | 15 minutes |
| **Ways to avoid social engineering**<br>Review the list of ways to avoid social engineering.<br>Pause to see if anyone has anything else to add or any questions. | Slides 13 through 15 | 10 minutes |
| **Discussion: Approaches for avoiding social engineering**<br>Break your learners into small groups.<br>Have your learners brainstorm ways to avoid social engineering and record their thoughts on their guided handouts. | Slide 16, Handout | 10 minutes |
| **Wrap up, final tips, and final questions**<br>Review the closing thoughts and share the suggested resources.<br>See if anyone has any final questions. | Slides 17 through 20 | 5 minutes |

## Considerations

Social engineering is an interesting and complex topic that has the potential to generate a lot of discussion and questions. You might consider leaving extra time and space for learners to discuss this topic, share examples that they have encountered, and unpack strategies for dealing with social engineering.

There is a good deal of information out there on social engineering and many of your learners might find the topic particularly interesting. You might want to share additional resources and emphasize ways to learn more.

## 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 phishing schemes, spam, and scams via email, text, and phone calls.

Additionally, this module can be connected in interesting ways with modules on data minimization and data generation, since social engineering uses manipulative techniques and knowledge about you to trick you.

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 the guided handout. However, given how much content is here, 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 social engineering?

A. A technique used by advertisers to get you to buy a product
B. Strategies used by cybercriminals to convince you to engage in questionable behavior, such as revealing your personal information or sending money
C. The ways in which social media sites influence your communication style
D. A form of going viral on social media

What is not an example of a social engineering technique?

A. Baiting or luring someone in with false promises
B. Phishing schemes or tricking someone into doing something with a false sense of urgency
C. Pretexting schemes or impersonating a trusted source to fool someone
D. Spyware or a type of malware that can live on malicious websites

What should you not do to avoid social engineering?

A. Call out the scammer and tell them to leave you alone
B. Know how to identify phishing schemes and other kinds of scams over text and email
C. Investigate requests, especially if they seem overly urgent or are pressuring you to do something
D. Keep your accounts and information secure with things like multi-factor authentication

True or false: Social engineering can only happen online.

A. True
B. False
C. Unsure

## Answer Key

What is social engineering?

*Answer: B, Strategies used by cybercriminals to convince you to engage in questionable behavior, such as revealing your personal information or sending money*

Social engineering are different types of manipulative techniques and strategies aimed at tricking people into performing questionable or ill-advised acts, such as breaching their personal security, giving away their data or information, or sending money. Social engineering is a hallmark of things like phishing schemes and scams.

What is not an example of a social engineering technique?

*Answer: D, Spyware or a type of malware that can live on malicious websites*

Social engineering involves manipulation and trickery and takes the forms of things like phishing schemes, false promises, or impersonation. Malware tends to be more stealthy in nature and doesn't involve the techniques commonly seen in social engineering scams.

What should you not do to avoid social engineering?

*Answer: A, Call out the scammer and tell them to leave you alone*

The techniques used to avoid schemes and scams and overall digital security best practices can all help you avoid social engineering methods. Directly engaging with scammers is not recommended. It's better to just ignore them and report them if needed.

True or false: Social engineering can only happen online

*Answer: B, False*

Social engineering has a long history dating back centuries! Social engineering scams used to happen in-person or involve communication technologies like letters. The social engineering techniques we see today are all quite old and have just been adapted for the internet age.

## 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
1.1 Data Generation Online

1.2 Data Minimization
1.2 Password Hygiene

1.3 Data Breaches
1.3 Social Media Account Hacks

2.2 Social Media Settings

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.