Multi-Factor Authentication

Facilitation Guide

Introduce learners to one of the best options for keeping accounts and information secure online.

Overview

This lesson will introduce learners to multi-factor authentication, including what it is, why it is useful, and how to begin using it on different apps and sites.

For more information, be sure to watch Series 1, 3, and 4 of NYC Digital Safety videos.

Outcomes

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

- Define multi-factor authentication
- Describe ways to enable multi-factor authentication on different apps and sites
- Name the benefits of using multi-factor authentication

Format + Time Frame

This lesson provides an informational overview of multi-factor authentication and a how-to guide for setting up and using multi-factor authentication on different sites.

This lesson will take approximately 15 to 20 minutes. With optional activities, this lesson can extend to about 30 minutes.

Materials

Materials needed for this module include:

- 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
Overview of MFA Provide a brief overview of MFA and highlight some of the forms MFA takes and how to get started with using MFA. Pause for any questions.	Slides 3 through 5	8 minutes
Activity: Considering your sites and security needs [optional] Give learners the guided handout. Have them list out accounts they use frequently and make a plan for checking on whether or not MFA is available. Have them check on a few accounts to see if there's an option for MFA.	Slide 6, handout	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 7 and 9	5 minutes

Considerations

Depending on your audience and how you'd like to deliver this content, you might consider doing a more hands-on walkthrough and demo of how to set up multi-factor authentication on a popular website, such as a Google account.

You might find that most attendees are fairly familiar with the concept behind multi-factor authentication, so depending on your audience you can have time for more hands-on activities or to bring in other, related digital security content for more extended experience.

Options and Variations

You can combine this lesson with other, related lessons on privacy and security settings for a longer workshop experience, from a half hour to a full hour or more. Additionally if you are delivering this content via a workshop, you can opt to share the information and have patrons set-up multi-factor authentication on their own, or leave some extra time to walk patrons through the set-up process with a sample site or app that most attendees use.

The information here can also easily be delivered to patrons at service points via the provided 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 multi-factor authentication?

A. A layered approach to security where a system require a user to produce two or more credentials to verify their information and identity
B. A way of safely storing passwords
C. A method of encrypting passwords
D. Another term for captcha images on websites

Where can you implement multi-factor authentication?

A. Your bank account
B. Your email account
C. Your social media accounts
D. Work and business accounts
E. All of the above

Which of the following is NOT a multi-factor authentication methods? Select all that apply.

A. A PIN number
B. A code you receive via SMS text
C. A fingerprint
D. A username
E. A security question that you answer

Answer Key

What is multi-factor authentication?

Answer: A, a layered approach to security where a system require a user to produce two or more credentials to verify their information and identity

MFA refers to using multiple credentials in order to login to an account, rather than just entering a username and password.

Where can you implement multi-factor authentication?

Answer: E, all of the above

MFA is available in many places now! Places like banks, email accounts, workplaces, etc. frequently offer, or even require, MFA.

Which of the following are multi-factor authentication methods? Select all that apply.

Answer: D, a username

MFA uses token, biometrics, knowledge, or a device you have on you, such as a phone, for that extra credential. Your username wouldn't be considered an example of MFA.

Connections to Other Modules

This module connects 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!

1.2 Password Managers
1.2 Password Hygiene

1.3 Data Breaches
1.3 Social Media Account Hacks

2.2 Social Media Settings

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

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.