NYC Digital Safety
Privacy & Security

Password Hygiene

Facilitation Guide

Introduce learners to best practices around password hygiene and empower them to better manage their passwords and online account security.

Overview

This module introduces learners to various best practices around password hygiene and instructs them on different steps and actions they can take to better manage their passwords and to secure their online accounts.

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 password hygiene
- Discuss the benefits of practicing password hygiene
- Provide examples of best practices and methods to manage and secure passwords

Format + Time Frame

This module provides an informational overview of password hygiene and a how-to guide for implementing different password hygiene best practices. Materials include the following:

This module will take approximately 35 minutes. With optional activity, this module can extend to about 60 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
Define password hygiene Provide a brief definition of password hygiene and see if anyone has any questions or anything to add. Briefly share reasons why password hygiene is important.	Slides 3 and 4	5 minutes
Overview of strong passwords Share suggestions and tips for writing a strong password.	Slides 5 and 6	8 minutes
Activity: Password TLC [optional] Have learners work through the guided handout to review and brainstorm updates for their passwords, using the suggestions and tips listed.	Slide 7, handout	10 minutes
Overview of creating strong passwords Share different techniques for creating a strong password.	Slides 8 through 11	10 minutes

Pause after each technique to see if learners have anything to add.		
Activity: Create your own strong password [optional] Have learners use the guided handout to practice creating their own strong passwords.	Slide 12, handout	15 minutes
Overview of ways to store and secure passwords Review tips for protecting and storing passwords. See if learners have any other suggestions.	Slide 13	5 minutes
Wrap up, final tips, and final questions Review the closing thoughts and share the suggested resources. See if anyone has any final questions.	Slide 14 through 16	5 minutes

Content Variations

This module works very well in conjunction with other modules and activities around password management and online account security best practices. You can combine this module with a variety of other ones on passwords for a more extended workshop experience, or have your learners complete an optional activity.

However, if you have more limited time, this module provides a strong foundation in password management best practices. You could consider running a shorter workshop that focuses on this module and provide your learners with guided handouts from other password modules for them to further develop their skills and knowledge on their own.

Consider extending your learning experience by leaving additional time for your learners to explore different aspects of password hygiene, to develop plans for their overall password hygiene, or to begin testing out different password hygiene methods.

You can also provide this information to patrons via a service point by briefly introducing them to what password hygiene means and providing them a copy of the handouts for Password Hygiene, Multi-Factor Authentication, and Password Managers.

Considerations

Password hygiene might be a new term for many in your audience, so make sure everyone is clear on the term and what it does and does not entail. Depending on your audience and how you'd like to deliver this content, you might also consider leaving additional time for individual exploration and activity to help your learners get started with implementing password hygiene best practices.

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 password hygiene?

A. Organizing and cleaning up your list of stored passwords
B. Deleting old accounts that you no longer use
C. Never sharing your passwords with others
D. Using different methods to select, manage, and secure your passwords

What is a method that you should not use to manage your passwords?

A. Use a password manager tool to safely store your passwords
B. Create unique and long passwords
C. Write your passwords down and store them somewhere so you don't forget them
D. Do not use personal information in your passwords

How confident do you feel about your overall online account security?

A. Confident - I've taken steps to ensure my accounts are security
B. Not confident - I'm concerned about my security
C. Not sure - I feel like I could do more

Answer Key

What is password hygiene?

Answer: D, Using different methods to select, manage, and secure your passwords

Password hygiene involves multiple methods, approaches, and best practices.

What is a method that you should not use to manage your passwords?

Answer: C, Write your passwords down and store them somewhere so you don't forget them

Managing passwords can involve multiple different steps and aspects and includes both creating and storing passwords in a strong and secure way. The incorrect answer here, writing passwords down, is considered risky even if you are taking the passwords offline. The passwords would be overly exposed and vulnerable if they are just written down for anyone to potentially see.

How confident do you feel about your overall online account security?

Answer: personal opinion, so no correct answer!

Note that you can use this question as a pre-test question and use it to generate discussion in your workshop.

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!

1.2 Data Minimization
1.2 Multi-Factor Authentication
1.2 Password Managers

1.3 Data Breaches
1.3 Social Media Account Hacks

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.