Learning Objectives: Passwords



# Module Learning Objectives

This purpose of this document is to identify and document the learning objectives of this training module. This information determines the contents of the training module, regardless of how it is communicated.

**Title**: Passwords and Password Managers

### Target Audience

All faculty, students and staff with computer access.

### Goal

Course participants will learn the need for good password practices. They will be able to define what makes a good password. They will also learn how to manage and maintain passwords securely. Because passwords are often the first, and sometimes only, line of defense secure password management a critical practice.

### Background

Passwords are a fundamental element of security for an overwhelming number of computer systems and applications. Choosing passwords and protecting them is critical. This module discusses how to choose passwords including using passphrases, using different passwords on different systems, and how to safely manage those passwords using password managers.

### Learning Objectives

1. Learners can explain the need for strong passwords.
   1. *Individual Metric*: *Learner correctly identifies reasons strong passwords are needed in a test question or interactive training session.*
2. Learners can explain why single dictionary words are poor passwords.
   1. *Individual Metric*: *Learner correctly identifies reasons dictionary passwords are poor in a test question or interactive training session.*
   2. *Organizational Metric*: *A password assessment against a sampling of user passwords*.
3. Learners can explain what a passphrase is and demonstrate how to create one.
   1. *Individual Metric*: *Learner correctly identifies strong passphrases in a test question or interactive training session.*
   2. *Organizational Metric*: *A password assessment against a sampling of user passwords*.
4. Learners can explain why you need to use a unique password for every account.
   1. *Individual Metric*: *Learner correctly identifies reasons passwords should not be reused in a test question or interactive training session.*
   2. *Organizational Metric*: *A password assessment against a sampling of user passwords from multiple systems to see if the same user reuses them*.
5. Learners can demonstrate how password managers work and the benefits of using them.
   1. *Individual Metric*: *Learner correctly identifies what password managers are and their benefits in a test question or interactive training session.*
   2. *Organizational Metric*: *Use SCCM or similar tool to identify the number of password manager tools installed on systems*.
6. Learners can explain the reasons to be careful when choosing password reset questions and answers.
   1. *Individual Metric*: *Learner correctly identifies the dangers of choosing password reset questions and answers that can easily be looked up or guessed in a test question or interactive training session.*
   2. *Organizational Metric*: *Assess a sampling of user password questions and answers*.
7. Learners explain the risks involved using untrusted systems or systems for logging in.
   1. *Individual Metric*: *Learner correctly identifies what untrusted systems are and the risks of using them in a test question or interactive training session.*
8. Learners can identify the benefits of 2 step authentication and some of the options commonly used.
   1. *Individual Metric*: *Learner correctly identifies various types of 2 step authentication and their benefits in a test question or interactive training session.*
   2. *Organizational Metric*: *Survey the number of community members who say they are using 2 step authentication for sites like Gmail*.