Lesson Plan—Protecting Your Passwords

# General Description

Passwords are an important part of our daily lives, as they control access to our banking, social media, email, and grades. Students need to know the basic methods attackers can use to steal their passwords and accounts, and how they can defend their accounts from attack.

# Time Allowed

This lesson can be completed in roughly 10 minutes if there is no assessment or lab exercise. The lesson could easily be expanded to a full class period with the addition of a lab/demonstration and a short quiz.

# Learning Objectives

The optional objectives list the term the security industry uses to describe these mistakes or attacks, but they should not be used for assessments unless the students are in a course that leads to a security certification. In general, the students just need to be able to explain the concepts.

## Overall Objective

The overall objective of this class is that students realize they need to begin using password managers and two factor authentications.

## Common password mistakes

1. Students will understand that short or easily guessed passwords can allow attackers to access their accounts.
2. Students will understand that using the same password for multiple accounts can allow an attacker to compromise all their accounts if they get the password for one account.
   1. Optional objective. Students will know that the term for this mistake is Password Reuse.

## Common password attacks

1. Students will know that know that an attacker could try combinations of words in a dictionary of common passwords to guess their password.
   1. Optional objective. Students will know that accounts should be locked after a certain number of failed logins to defend against this.
   2. Optional objective. This method is called a “brute force password attack”
2. Students will know that lists of usernames and passwords from hacks of well-known web sites are easily available. If the student uses the same username/password on all their sites, attackers may be able to break in to all their sites.
   1. Optional objective. This attack is called “credential stuffing.”
3. Students will know that if they use a public or a friend’s computer, and it has been compromised (hacked), any usernames/passwords they use on that computer will be compromised.

## Common defenses

### Password Selection

1. Students will understand that they should select long passwords, or passphrases
2. Students will understand that they should use a different password for every site.

### Password Managers

1. Students will understand that password managers will help them keep track of many long passwords, with a separate password for every site.
   1. Optional objective. Students will know that a password manager will usually be able to select and store long random passwords for them.

### Two Factor Authentication (2FA)

1. Students will know that, while not perfect, 2FA provides their most secure option.
2. Students will know that 2FA sends a number to their phone, which must be used to complete the login.