Activity 13-01: Create a Strong Passphrase

Big Idea

You may have been taught that to create a strong **password** you need to use at least eight **characters** making sure you include at least one number, one **special character** (like @, #, or !), and a mix of upper- and lower-case letters. Unfortunately, that advice is outdated. Criminals don't usually try to guess your passwords anymore. They use password-cracking software that can quickly figure out short passwords regardless of which characters you use.

Current password recommendations include using a passphrase. A **passphrase** is a longer string of words that still uses numbers and special characters that makes it harder for someone to figure out using software. Passphrases are 14, 16 or more characters. Some IT personnel will create much longer passphrases to protect critical resources, but they probably use **password-manager software** to help keep track of them. The length of your passphrase is more important than the characters you use. Longer is harder to crack.

Materials

- Web browser and Internet connection

Vocabulary

Password
Characters and special characters
Passphrase
Password-manager software

Background

Your passphrase should not contain a word that can be found in a dictionary, in *any* language. If you include common words, names, places, sports teams--any word, actually--it's easier to crack. For example, the word *animal* is found in the dictionary but if you change it to *an1m@l*, that combination of characters is not found in any dictionary and harder to crack.

Think of it this way:

- If you use only lower-case letters, there are 26 possibilities for each character

- If you use both lower- and upper-case letters, you've doubled the number of possibilities for each character to 52.
- Including numbers increases the possibilities for each character to 62
- Including special characters can add about another 15 or so possibilities depending on the limits of special characters in your system.

To create and maintain a strong passphrase, **YOU SHOULD:**	To create and maintain a strong passphrase, **YOU SHOULD NOT:**

• Use different passphrases for every account or system.
• Match your passphrase to the value of what it is protecting. For instance, it is more important that your banking passphrase be extra secure compared to your library passphrase.
• Use the longest password or passphrase permissible. If that's way too long to manage, try to use passphrases that are at least 16 characters long.
• Use a mix of upper and lower-case letters, numbers, and special characters allowed by the system.
• Keep your operating system, browsers, and other software on your devices up to date. Updates include security protections.
• Use characters or numbers to substitute for letters in your password
  ○ $, S or 5 for s
  ○ 1, I or ! for i
  ○ @ or A for a
  ○ 7 or T for t
  ○ 3 or E for e
  ○ 9, G or 6 for g
  ○ 0 or O for o
  ○ 8 or B for b
	• Use common phrases, famous quotations, song lyrics, birthdays, or other commonly guessed phrases or information. The two most common passwords are *password* and *123456*. Is one of those one of yours?
	• Use simple patterns of letters (*abcde*) or numbers (*12345*).
	• Use private information in your passphrase like your phone number, your name, or your address.
	• If you use personal information in your passphrase, don't post about it on social media. For example, if you use your pet's name as your password and then post pictures and his/her name on social media, you're giving people information to guess your password.
	• Reuse a password or passphrase!
	• Write it down, anywhere.
	• Share your passphrase with anyone. The possible exception to this is if you are dealing with older or very young people. They may want to let their family know their passphrases in case they forget them.

Activity Directions

So…all you have to do is use 16 or more characters, varied, with no real words. Simple, huh? Well, there are some steps you can take to make it easier.

1. Begin by visiting this site to see how long it might take to crack one of your own passwords: https://www.security.org/how-secure-is-my-password/
    a. If you don't want to input your own password, consider trying the following:
        i. The word *Password*
        ii. *123456*
        iii. *Changeme*
    b. You can also play around and see how making minor changes can increase how long it might take to crack a password. For example, try the following:
        i. Enter a common word, like *football*. Not so great, huh?
        ii. Add a capital letter. Try *footBall*. A little better.
        iii. Change it up by using some numbers instead of all letters, like *f00tBall*. Getting better.
        iv. And a special character, like *f00tB@ll*. Even better.
        v. But make it just two characters longer, like *f00tB@ll97*. Wow! Much better.

That was using a fairly short password with only 8-10 characters. Getting up to 14 or 16 will make it even stronger. One way to do that is to generate a starting point with four simple words that have some characters changed up to eliminate common words.
Try the following steps and see what you come up with:

Step	Outcome
Look around the room and identify four objects. Or create a four-word phrase that is easy for you to remember. You want about 16 characters or more total.	You see your cat sitting on your desk next to your phone, a framed photo, and on top of a book. cat, phone, photo, book
List the phrase in any order with upper- and lower-case letters. Even though these are common words, the length of the passphrase makes it stronger.	CatPhonePhotoBook

To make it stronger, you can respell some words phonetically or replace some letters with numbers or special characters.	Kat4onnPho2Buuk!