### Web Literacy Competencies

Privacy Security

### Audience

- 13+
- Beginning account holders

### Materials

- Computer
- Internet Access
- Pen and Paper
- Dictionary
- Dice
- Survey
- Survey Incentive

### Learning Objectives

- Make more or less secure passwords and explain what makes them secure
- Judge a passwords security strength based on key indicators
- Collect original research on passwords

### How learners become mentors

- Shadow a student or less experienced facilitator so they can practice leading this activity.
- If some students move faster or are more confident in the activity, ask them to peer mentor another group.
- Conclude by prompting students to teach this activity to their friends and family.

### See community remixes

Check out the ways educators and activists have modified this activity for their specific audiences in our Discussion Forum.

# Section 2. Writing the Web

## Draw Secure Passwords

Made by Stacy Martin and the Mozilla Privacy Team. Remixed for Clubs by Mozilla.

**Learn about pass-phrases, pronounceable and random passwords** using generators. You will **find out what you can do to create better passwords**, and explore different types of passwords to learn about their pros and cons.

45 minutes – 1 hour

## Preparation

**Do the activity on your own** to become familiar with it.

## Draw a passphrase

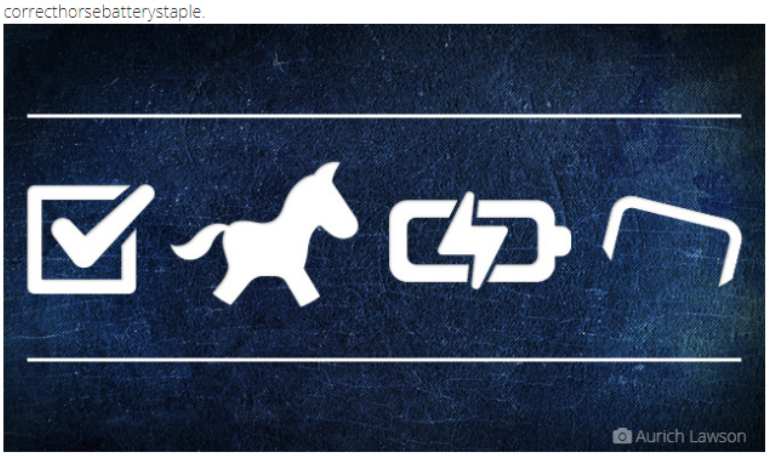
20 min

Pass-phrases are random combinations of four common words. They tend to be hard to guess, but easy to remember.

XKCD

- Try this passphrase generator.
- You can also do this **offline** by selecting four random common words from the dictionary and putting them together. Discuss what you can do to make sure the words are really random.
- Now try noun, verb, adjective, noun.
- Try Diceware, which provides a list of almost 8,000 English words, preceded by 5 digit numbers. You roll a pair of dice 5 times and add the corresponding word to your passphrase. Repeat several more times to add more words and make your password less crackable.
- Which passphrases are easier to remember? Why?
- Which might be easier to guess? Why?

**Draw yourself a picture** to help you remember your passphrase. This one is correcthorsebatterystaple.




## Remember a pronounceable password

5 min

Create a **pronounceable password** by using this password generator and selecting "pronounceable." These tend to be easy to remember and harder to crack because they do not contain words that can be found in the dictionary. Wait 5-10 minutes (go on to the next step and then come back) and without looking, write the pronounceable password you generated. Were you able to remember it?

## Remember a random password

5 min

Create a **random password** by using this password generator and selecting "random." These are harder to crack, but also harder to remember. Wait 5-10 minutes (go on to the next step and then come back) and without looking, write the random password you generated. Were you able to remember it?

## Basic 8, Basic 16

10 min

Create at least one **basic 8** (must have at least 8 characters) password and at least one **basic 16** (must have at least 16 characters) password. Discuss and brainstorm a list of good practices when creating strong passwords, using the questions below and what you've learned from the exercises above.

- Should you add one or more digits (numbers)? Did you know that if you put a digit at the beginning of your password, it's better than no digit, but not as good as having a digit in the middle?
- Should you add one or more symbols? Did you know that of 32 symbols, most people use the exclamation point, so if you use a less popular symbol, your password may be harder to guess?
- Should you use a mix of capital and lower case letters? How can this help make your password harder to guess?
- Have you tested the strength of your passwords using a password meter?

## Do your own password research

20 min

Create a **password survey**. In exchange for a cookie or a candy bar, ask others for information about their passwords. Don't ask them for their actual passwords, but ask questions such as these listed below. Feel free to add additional questions of your own. Track your results in a spreadsheet. What did you learn? Discuss and compare.

Sample Survey Questions:

- How long is your password?
- Does it have a digit?
- Does it have a symbol?
- Do you write your passwords down?
- Do you reuse your passwords?