Creating strong passwords
40 minutes

L E S S O N P L A N

Background	This is a module that can be inserted into other lessons for various topics and audiences. This module does not delve too far into why strong passwords are important because it would likely be part of a larger class or series on data security.	
Materials	Sets of 5 dice, diceware word list, handout with diceware instructions	
Threshold Concept frame & learning outcomes	Information has value - Students will be able to explain criteria for strong passwords. - Students will create a strong passphrase using diceware. - Students will see a demonstration of a passphrase used with a password manager.	
Introduction	Introduce myself, go around and have students say their names. Goals of the session: 1. Figure out what makes for a strong password 2. Practice creating a passphrase using diceware 3. See how to use a passphrase with a password manager	**Time** 5
Discussion	I think most of us have probably heard advice at one time or another about what makes for good strong passwords. What advice have you heard? [Write down the things that are said.] Do you agree or disagree with these pieces of advice? What makes these rules easy or difficult to follow? So, the two main things that make for a really good, strong password are randomness and length. Our brains are hard-wired to think in patterns, and it is really, really difficult for us to fake randomness. I'm going to show a short video that illustrates this [Khan academy entropy video 2:09]: https://youtu.be/vVXbgbMp0oY	**Time** 15

Diceware activity	We know, based on tests of password cracking software, that long, random passwords are strongest, and we also know that 1) it's really hard to remember long strings of random characters and 2) humans are pretty bad at faking randomness. There's a method called diceware you can use to create a really good, strong, random passphrase—rather than a single password—that you can probably memorize. You have sets of 5 dice and a printout [or link to PDF, if it's in a computer lab] of a long, numbered wordlist. [Demo the steps below and give out a handout with the same instructions, link to the dice ware word list, spaces for 6 5-digit numbers and their corresponding words, and a few lines for writing a mnemonic.] 1. Roll the five dice and write down the numbers that you roll, left to right. 2. Repeat this 5 more times, for a total of 6 5-digit numbers. 3. Using the wordlist, look up the word that corresponds to each number and write it down. Once you're found your passphase, keep it to yourself. There's a space on your handout that you can use later on to create a story or mnemonic for yourself to help remember your passphrase.	**Time** 10
Password manager	Questions? OK, now that you've created passphrases, do you see any potential difficulty to using this method for creating passwords? [Ideally someone will say that it would be tough to remember these for every site; otherwise, suggest this]. Security experts recommend using a strong passphrase with a password manager program that will generate unique, random passwords for all your different accounts so that you're not reusing the same passwords again and again. Your passphrase then becomes your master password, and the password manager takes care of remembering everything else. Demo a password manager. Time for questions.	**Time** 10
Learning Assessment End of Class	Were students able to create passphrases? Was there a substantial discussion? Did they seem to "get it?"	
Things to Remember for Next Time		