**Discussion: Could you guess your best friend’s password?**

How do you come up with your passwords? Do you think other people use the same method? How many guesses do you think it would take for you to figure out your friend’s or partner’s email password?

**Background Info: A secure password needs to be random, long and unique**

Some attackers can make billions, or even hundreds of billions, guesses about your password per second!

The best way to keep them from guessing your password is to make it random, long (a pass*phrase* not a pass*word*), and unique.

**Activity #1 for making a random and long passphrase: The book method**

1. Grab any book off of the shelf.
2. Close your eyes
3. Open your book to a random page
4. Put your finger somewhere on the page
5. Open your eyes and write down the word closest to your finger.
6. If the word is a very common (easy to guess) word, go back to step 1.
7. Repeat steps 1-6 six more times, giving you a total of seven words.
8. Voila! You have a new passphrase.

**Activity #2 for making a random and long passphrase: The dice method**

Grab a pair of die and [click here to visit the Electronic Frontier Foundation’s long word list](https://www.eff.org/files/2016/07/18/eff_large_wordlist.txt).

1. Roll the die 5 times. Write down the number you roll each time. \_\_ \_\_ \_\_ \_\_ \_\_
2. You now have a five-digit number. Find that five digit number. Write down the word next to that number. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
3. Repeat steps one and two 6 more times, giving you a total of seven words. (If you have more dice at home, you can roll more than one at a time. That will make the activity go faster!)

**Activity: Memorize your passphrase**

Come up with a story, scenario, or sentence that you will be able to remember and that can remind you of the particular words you chose, in order.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

If you’re struggling, try this too:

Write the passphrase down on a sheet of paper, and keep it someplace safe. When you type in your passphrase, try to remember it without looking. Then check to see if you were right by looking at the paper. When you can get it right every time, destroy the paper.

**Activity: Use a password manager to make passwords unique**

A password manager is a tool that creates and stores passwords for you, so you can use many different passwords on different sites and services without having to memorize them. You only need to remember one random and long passphrase that allows you to access the password manager.

**Is a password manager a good idea for you?** Using a password manager creates an obvious target for hackers, and a single place where all your passwords are stored. On the other hand, can you remember a unique, random and long password for every single site you log in to?

[Follow the steps to create a KeePassXC account](https://ssd.eff.org/en/module/how-use-keepassxc).

**Wrap up discussion: Changing habits**

Do you think you’ll manage your passwords differently after this class? Why or why not?

**For further study:**

Making secure passphrases with the Diceware method: https://theintercept.com/2015/03/26/passphrases-can-memorize-attackers-cant-guess/

Tactical Technology Collective’s Security-in-a-Box: https://tacticaltech.org/projects/security-in-a-box-key-project/

**Notes:**