Passwords: intermediate

Even though it's one of the most important things you can do for your online security, creating and using strong passwords can be a tough sell for learners. Secure password advice can conflict, and it's hard to remember and implement when all you want to do is create an account and start using it! In this lesson, we'll look at ways to explain the "how" and "why" behind strong passwords.

Recommended Reading

- Creating Strong Passwords
- Animated Overview: How to Make a Super-Secure Password Using Dice
- Using Password Managers to Stay Safe Online
- XKCD comic about password strength and diceware passwords

Gotchas and Other Problems You Might Hit

- When making new passwords, there may be a few participants who will forget their new passwords. If people have changed the passwords for critical accounts or for their devices without memorizing their passwords, this activity may cause more harm than good.
- Consider suggesting people write down their passwords (on paper or in password managers). For those who write down their passwords, remind them to watch out for others peeking at their papers, and to keep these papers in a safe place!
- It is also worth looking into memory retention techniques for those who have trouble remembering their passwords, like mnemonics, creating illustrations or imagery to accompany the password in the course of their memorization, creating a funny story around the password, and so on.
- Some people may have trouble with typing long passphrases due to motor difficulties. If this is the case, provide accommodations for them to still participate, but perhaps loosen requirements on the exact number of words for the passphrase.
- Others may have trouble with a passphrase generated from the diceware or random dictionary word selection technique, perhaps due to issues with being able to spell the word. Consider making an accommodation by helping them to choose another more familiar, but still sufficiently random, word.

Learning Objectives

Learners will:

- Be able to explain why the randomness of using dice or a book is effective at producing a secure **passphrase**.
- Produce a highly secure passphrase.

Ratio

Instructor: Learners
1:4

Suggested Materials

The facilitator may want to provide post-its and pens, for participants to (optionally) write down their new passphrases.

Optional: books

Optional: dice

Optional: EFF's dice wordlist

Relevant Articles

Lesson Content

Knowledge Share

Review: Walk learners through why bad passwords are easy to guess.

- Common English words
- Common English words with some letters turned into numbers
- Names and dates
- Patterns on the keyboard (even ones you think are clever)
- Show list of most popular passwords: https://en.wikipedia.org/wiki/List_of_the_most_common_passwords

Other points you can cover include:

- Show examples of really strong passwords.
- Discuss why you should never reuse a password for multiple sites or services.
- Discuss why a **password manager** is useful.
- Discuss the purpose of a **master password** or passphrase.
- Discuss remembering a passphrase.

Activity: Generate a Passphrase

There are a few options for leading participants through the process of creating a passphrase. One nice thing about these activities is that learners can participate in them even if they didn't bring a computer or other device.

The following activities require learners to remember their new passphrases. Memorization is not realistic for everyone, and people may forget their new passphrases after the workshop. It may be useful to provide post-its and pens for learners to write down their new passphrases.

The facilitator may want to follow up with suggestions for memory-recalling measures, like using mnemonics (e.g. "**E**lephant **R**ainbow **N**ovel" can be remembered by "**ERN**"), or creating a visual story around the passphrase (e.g. "I remember 'Elephant Rainbow Novel' by imagining an elephant walking on top of a rainbow, and reading a book at the end of the rainbow").

Word selection from books

One option simply requires that you have a book for each learner, which makes it a great option for trainings in schools, libraries, or other places with a lot of books sitting around.

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

Knowledge share: Passphrase Generation with Diceware (optional)

Another option for creating a passphrase is a system called Diceware, where you use a set of 5 dice and a predetermined word list to generate a passphrase. We're big fans of Diceware at EFF. We even created our own customized EFF dice set and our own word list. It can be a lot of fun for users with a certain kind of geeky sensibility.

That said, Diceware can also be intimidating for some participants. If you don't have several sets of dice and word lists on hand, it can create an awkward lull while everyone is waiting for their turn.

Instructions for running a Diceware activity and using the list is found at eff.org/dice.