HOW TO BUILD A GREAT PASSWORD

SAFETY > 4.1 PROTECTING DEVICES

TARGET GROUP	AGE GROUP	PROFICIENCY LEVEL	FORMAT	COPYRIGHT	LANGUAGE
School drop outs, Students (primary school), Students (secondary school)	Children, Teenagers	Level 1	Activity sheet	Creative Commons (BY-SA)	English, French

Participants learn the importance of creating a strong password, how to do so, and how to make sure it stays private after they create it. They will be taught to create passwords that are easy to keep in mind but difficult to guess at the same time. This resource forms part of the “Cyber Heros” learning programme designed for 8 to 14 year olds.

General Objective	Skillset building
Preparation time for facilitator	less than 1 hour
Competence area	4 - Safety
Time needed to complete activity (for learner)	0 - 1 hour
Resource originally created in	French

WORKSHOP DIRECTIONS

1 Goals for students

- Recognize the importance of never sharing passwords, except with parents or guardians.
- Understand the importance of screen locks that protect devices.
- Know how to create passwords that are hard to guess, yet easy to remember.
- Choose the right security for their login settings, including twofactor verification

2 Let's talk

Better safe than sorry

Digital technology makes it easy for us to communicate with friends, classmates, teachers, and relatives. We can connect with them in so many ways: via email, text, and instant messages; in words, pics, and videos; using phones, tablets, and laptops. (How do you
connect with your friends?)
But the same tools that make it easy for us to share information also make it easier for hackers and scammers to steal that information and use it to damage our devices, our relationships, and our reputations.
Protecting ourselves, our info, and our devices means doing simple, smart things like using screen locks on phones, being careful about
putting personal info on unlocked devices that can be lost or stolen, and, above all, building strong passwords.

• Who can guess what the two most commonly used passwords are?
(Answer: “1 2 3 4 5 6” and “password.”).

• Let’s brainstorm some other bad passwords and what specifically makes them bad.

(Examples: your full name, your phone number, the word “chocolate.”)
Who thinks these passwords are good?

3 Activity

Here's an idea for creating an extra-secure password:
• Think of a fun phrase that you can remember. It could be your favorite song lyric, book title, movie catchphrase, etc.
• Choose the first letter or first couple letters from each word in the phrase.
• Change some letters to symbols or numbers.
• Make some letters uppercase and some lowercase.
• Let's practice our new skills by playing the password game

1. Create passwords
We'll split into teams of two. Each team will have 60 seconds to create a password. (Challenge option: Students share clues with the class first to see how much contextual information the class needs to be able to make an accurate guess.)
2. Compare passwords
Two teams at a time will write their password on the board.
3. Vote!
For each pair of passwords, we'll all vote and discuss whose is stronger.

4 Takeaway

It's important and fun to create strong passwords.

5 Guidelines for creating strong passwords

Here are some tips for creating passwords to keep your information safe.

Strong passwords are based on a descriptive phrase or sentence that's easy for you to remember and difficult for someone else to guess – like the first letters in words that make up a favorite title or song, the first letters of words in a sentence about something you did – and include a combination of letters, numbers, and symbols.

For example, "I went to Western Elementary School for grade 3" could be used to build a password like:

Iw2We$t4g3.
Moderate passwords are passwords that are strong and not easy for malicious software to guess but could be guessed by someone who knows you (for example, IwenttoWestern). Weak passwords commonly use personal information like a pet's name, are easy to crack, and can be guessed by someone who knows you (for example, "IloveBuddy" or "Ilikechocolate").

DOs
• Use a different password for each of your important accounts.
• Use at least eight characters. The longer the better (as long as you can remember it!).
• Use combinations of letters (uppercase and lowercase), numbers, and symbols.
• Make your passwords memorable so you don't need to write them down which would be risky

• Immediately change your password if you know or believe it may be known by someone other than a trusted adult.
• Always use strong screen locks on your devices. Set your devices to automatically lock in case they end up in the wrong hands.
• Consider using a password manager, such as one built into your browser, to remember your passwords. This way you can use a unique password for each of your accounts and not have to remember them all.

DON’Ts

• Don’t use personal information (name, address, email, phone number, Social Security number, mother’s maiden name, birth dates, etc.), or common words in your password.

• Don’t use a password that’s easy to guess, like your nickname, just the name of your school, favorite baseball team, a string of numbers (like 123456), etc. And definitely don’t use the word “password”!

• Don’t share your password with anyone other than your parents or guardian.

• Never write passwords down where someone can find them.