**AIM OF THIS SECTION:** Learn how to navigate the web safely

## 1. PERFECT PASSWORD

**20 mins**

**OUTCOME:**
**Learn how to create strong passwords**

**MATERIALS:**
**Paper, pencils, enough for all participants.**

### WHAT HAPPENS:

A good password uses a mixture of letters, numbers and symbols. It should be hard for someone to guess but easy for you to remember.

Take turns choosing a memorable object or a favourite phrase or saying, such as a line from your favourite book or film. Each person then thinks how to turn this phrase into a hard-to-guess but easy-to remember password with at least eight characters, using a mixture of letters, numbers and symbols. To help, draw a grid with two rows and as many columns as there are different letters in your password. If using a phrase, use the first letter of each word. Write the letters in the top row and a corresponding symbol or number below it.

For example, here the easy-to-guess word 'butterfly' becomes 'B@++3rf1Y', which is a much better password.

| B | U | T | T | E | R | F | L | Y |
|---|---|---|---|---|---|---|---|---|
| B | @ | + | + | 3 | r | f | 1 | Y |

Write a few passwords using this code, then give your passwords to a friend and see if they can decipher them.

**DISCUSS:** Can you think of any other ways to make a complicated password easy to remember? Where should you keep your passwords?

### SEARCH RESULTS

The key to a good password is finding a balance between something you can remember and something nobody else can guess. To be sure you've got a good password:

DO...

- Keep your password at least eight characters long.
- Use a mixture of upper and lower case letters, numbers and symbols.
- Use a different password for each account. Keep unique passwords for really important accounts like your email and social network.
- Log out when you have finished with an online service.

## 1. PERFECT PASSWORD (CONTINUED)

- Add a two factor authentication to your online accounts for an extra layer of security! That means that apart from entering your password, you receive a randomly-generated code to your mobile phone, which you have to provide to enter your account.
- Check your password strength by using tools such as The Password Meter, Kapersky Password Checker and All things Secured Password Checker

### DON'T...

- Only use words you can find in a dictionary.
- Include personal information such as your name or birthday.
- Use something obvious like '12345678', 'letmein' or 'password'.
- Enter your password into online forms or send it in emails. If you get an email from a website you use asking for your password, it's probably a phishing attempt and isn't really from that website. You can learn more about phishing and other security threats on page 58.
- Share your passwords with your friends. It doesn't mean you don't trust them, it's just good practice.
- Keep your passwords on display. If you need to write them down, keep them somewhere safe and out of sight, such as giving them to your parents. Don't keep them stored on your computer.

## TAKE IT FURTHER

## *BUILD THE STRONGEST*

7+

**20 mins**

**MATERIALS:**
**Paper & pencils for each team, signs or marks, digital device**

**TIP!**
Keep your password to yourself, and change it often.

### WHAT HAPPENS:

Form small teams. Each team makes up their own password and the opposing teams try to guess its strength. For example, the first team says 'bubble2007' and the other team guesses whether it's very weak, weak, good, strong or very strong, by running to respective signs or marks on a line along the ground.

You can then confirm the strength of the password using tools such as The Password Meter, Kapersky Password Checker and All things Secured Password Checker. You can play as many rounds as you like. The team that comes closer to guessing the strength of the most passwords, wins!