GUESS MY 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

In this workshop, participants get to understand the importance of possessing a strong password, and that it is possible for people with malicious intent to use quite a number of methods and software to guess their passwords.

General Objective	Awareness building
Preparation time for facilitator	less than 1 hour
Competence area	4 - Safety
Time needed to complete activity (for learner)	0 - 1 hour
Name of author	Nothing 2hide
Support material needed for training	Post-its in 4 different colours, Neutral post-its for noting colours and letters, One envelope per group, Pens
Resource originally created in	French

WORKSHOP DIRECTIONS

1 Introduction

This game-based workshop aims to demonstrate how to create a strong password. Through a combination of guessing and deduction, participants will understand that the more complex and long a password or code is, the more difficult it is to guess.

2 Beginning

When starting, it's important to emphasise the importance and usefulness of having strong passwords: Online for example, passwords protect access to all services. If a person of ill-intent guesses the password of an email address, they will be able to access that person's inbox. Passwords should be seen somewhat like padlocks that block people from getting into the box containing all a person's secrets. For this activity, you should ideally create groups of 2 sitting face to face. For the first step, give out the coloured cards, the 'ATTEMPTS' sheet and an envelope to every participant. The objective is to guess the other's password – contained in an envelope – in as few tries as possible.

3 Guess the colour

Explain to the children that they will have to choose a colour and place it in the envelope without their partner seeing. Once this is done, everyone will, in turn, need to guess the colour. This means a maximum of 4 attempts before the correct colour is found. Easy!

4 Guess the colour and the letter

Since the children will have found this very easy, choose again a colour but this time add a post-it with a letter ranging fro A to D (i.e. A or B or C or D) Now the same activity: everyone must in turn guess the combination chosen by their partner. When the guessing session is complete, ask what happened. They

will of course have needed more time to guess the content of the envelope. This is unsurprising since there are more variables and therefore more combinations. By adding an element, the time necessary to guess the code increases. Up to now it has been simple since they have guessed colour by colour and letter by letter.

5 Guess the combination

Repeat the same exercise but choose an order for their code. Repeat the same exercise but this time set an order for the code (for example GREEN + B, E + YELLOW, C + D, RED + BLUE). The partners will then have to try to guess the correct code in the right order at once. The children will quickly realise that this will take a very long time and they could well become frustrated at the process. This time, statistically, we do not add new elements but we do multiply the existing ones. Every variable of the code can be 1 of 4 colours OR 1 of 4 numbers. This results in 8 combinations. As there are two variables in the code, we multiply the number of characters themselves. 8^2 = 8 x 8 = 64 combinations.

6 The impossible combination

This time, add a to the code a third variable which will be a number between 1 and 4. The group will now have to guess a code comprised of 3 different elements and in the correct order. This will take much longer as there are: $(4+4+4)^3 = 12^3 = 12 * 12 * 12 = 1728$ combinations At this point in the activity, the participants will have understood that the more characters a password takes on, the larger the numbers of possible combinations and longer the length of time to guess it. According to the age group present, you can demonsrate the maths on the board.

7 Conclusion

The guessing sessions can stop now. The essential is that the participants have have understood the fact that the lengthier and more complex a password, the more solid it is. If there are computers are available, they can test any combination they wish with this password tester.