OFFLINE WORKSHOP - GUESS THE PASSWORD WITH HANGMAN

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

A group activity based on the game “hangman” that introduces participants to the importance of creating strong passwords.

General Objective	Knowledge acquisition
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	Thibault Dupiczak
Support material needed for training	Paper and Pens - Whiteboard (with pens) - 6 face dice (1 dice per group of participants)
Resource originally created in	French

WORKSHOP DIRECTIONS

1 Introduction

This group activity allows participants to explore the importance of creating strong and secure passwords. In addition to playing the game, it is important to explain to participants why it is necessary to secure their internet accounts, and provide them with tips on good practice so that they can do this for themselves.

Facilitation tip:

To learn more about passwords, we recommend that you look at the resource: Tool – passwords.

2 An Ironclad Password

To introduce the activity, begin by going around the table and asking participants what types of platforms they subscribe to (social media, video games, etc), how important they view the security of their accounts and what criteria they use to create their passwords.

3 Playing the Game

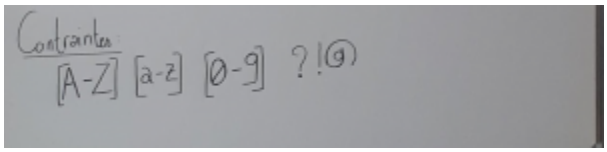
Next, divide the participants into 2 groups (making sure that the teams are made up of participants of different ages and backgrounds to ensure more interesting exchanges).

Each team makes up a password (conforming to certain restrictions such as type of characters, number of characters, etc). The password should contain 6 characters, 1 capital letter, 1 lowercase letter, and at least 1 number. The remaining restrictions are chosen by the facilitator.

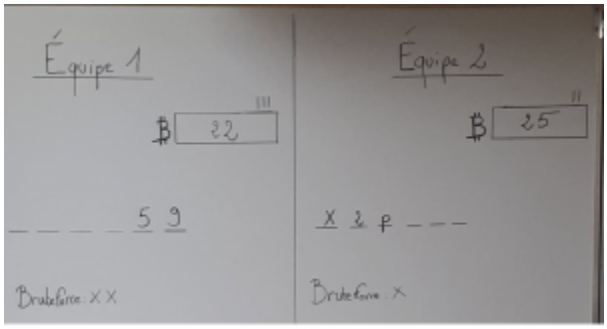
These additional restrictions are:

- A-Z] [a-z] [0-9] !?$
- [A-Z] [a-z] [0-9] !?$.-_

- [A-Z] [a-z] [0-9] !?$.-_@+



Then, decide on an amount that is the same for the 2 teams (30 bitcoins per team for example). Divide the whiteboard in two and write this amount on each side of the board. This amount signifies the number of points that each team has to play. On either side of the board, draw the number of blanks equivalent to the number of characters in each team's password (similar to the game 'hangman').



Each team then takes it in turns to try to guess a letter of the opposing team's password (again, similar to the game 'hangman'). The number of turns is limited to 10. At the end of the 10 turns, the team with the most bitcoins left in their account wins. If a team succeeds in guessing the other team's password, they steal all of the other team's bitcoins.

When a team guesses a letter, one bitcoin belonging to the opposing team is 'frozen' (this is represented by a line above the opposing team's bitcoin amount on the whiteboard). A 'frozen' bitcoin is *still counted in the account total* but *cannot be used* to perform an action.

Each team may choose one of the following actions:

- Guess a letter by chance (costing 2 bitcoins from the team who carries out the action)
- Use Brute Force* (costing 3 bitcoins from the team who carries out the action).

To effectuate 'Brute Force', one member of the team who wishes to carry out the action rolls the dice. If the result is higher than 3 (on a dice with 6 faces), the letter the team is trying to guess is automatically given to them by the opposing team

**Please see below for definition*

4 Feedback

Once the game is finished, the teams each reveal their passwords (if they have not been guessed already), and explain the various steps that they went through in order to create them. They may also provide their opinion on the method used by the opposing team.

Talk with the participants about the different methods they used to create their passwords (as well as the methods that they discussed at the start of the workshop). Provide them with information regarding password creation: how to create a good password, how to store their passwords, how to protect their accounts. You may also want to touch on password encryption (and may want to consider further workshops on this subject).

5 Definition

Brute Force: Brute force is one of the methods which may be used to discover someone's password. It consists of a piece of software (called Brute Force), which tries all of the possible combinations to crack a password (numeric, alphanumeric and special characters). When using this software, it is helpful to define certain parameters, in order to reduce the number of attempts needed to find the password (as this can be very time consuming). You can, for example, define a character limit or predefine certain character combinations. Indeed, it is possible to base a 'brute force' attack on information relevant to the person concerned (surnames/first names of close family or friends, date of birth, address, etc). In this situation all the possible combinations including these various criteria will be tried.