CREATING STRONG, UNIQUE PASSWORDS

SAFETY > 4.1 PROTECTING DEVICES

TARGET GROUP	AGE GROUP	PROFICIENCY LEVEL	FORMAT	COPYRIGHT	LANGUAGE
All, Job seekers, School drop outs, Students (secondary school)	Adults, Elderly citizens, Teenagers	Level 1	Activity sheet	Creative Commons (BY-SA)	English, French

This workshop will allow you to guide participants to create passwords that are:
a. Strong, because they are sufficiently varied and modified over time and
b. Unique, as they will be conceived through mnemonics created by the students themselves

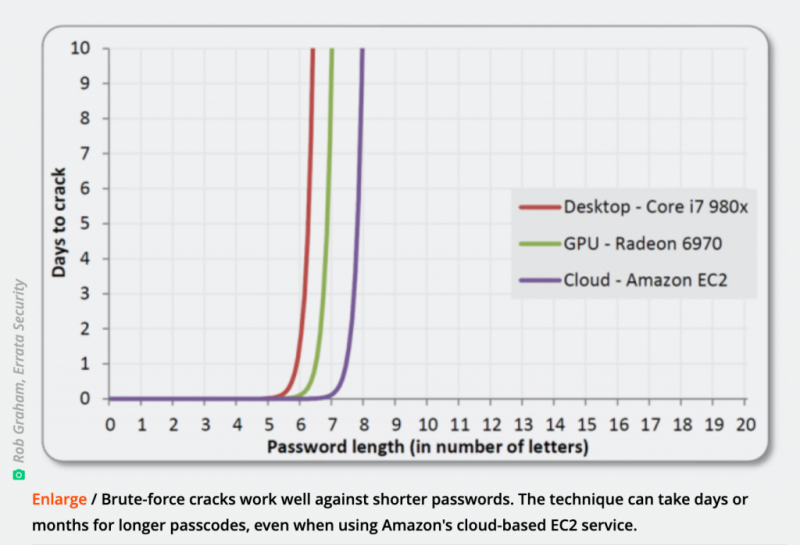
General Objective	Skillset building
Preparation time for facilitator	less than 1 hour
Competence area	4 - Safety
Time needed to complete activity (for learner)	0 - 1 hour
Name of author	André Van der Linden and Hélène Desmulliers
Support material needed for training	Paper, pencil, Optional: whiteboard projector, shredder (demonstrating that when it comes to passwords, we should leave no written trace!)
Resource originally created in	French

WORKSHOP DIRECTIONS

1 Guessing a number between 0 and 9

For this first step, each participant must choose in their head a number between 0 and 9 and have the group guess try to guess it. Time how long it takes for the group to find the number.

***Note*: participants will find the number rapidly – within seconds!** The longer the string of numbers, the longer the time it will take to crack the code.



Enlarge / Brute-force cracks work well against shorter passwords. The technique can take days or months for longer passcodes, even when using Amazon's cloud-based EC2 service.

https://arstechnica.com/information-technology/2013/05/how-crackers-make-minced-meat-out-of-your-passwords/2/

Here is how long it takes certain computers to break passwords of varying lengths. Note that this article was written in 2013 – computers will have only become quicker and even more adept at this.

2 Guessing a number between 0 and 999

As with the previous exercise, everyone should choose a number, this time between 0 and 999 – thus introducing more complexity. ***Note*: clearly it will take a lot longer for participants to guess the number. The ideal length of a cryptic code should be 12 characters or more!** The calculation speed of a computer is infinitely greater than that of a human brain. Also, according to Moore's law, the

speed of the microprocessors involved in the functioning of a computer doubles every year. This would be an interesting point to explain to the group.

***Facilitation tips**:* Refer here for more information on the subject.

3 Understanding what not to do

For this third exercise, the objective is to start building understanding of the logic of a password and what not to do when creating one. For this, you can print the labels below (or to remake them by hand on pieces of paper) and ask participants to link each personality to their password listed underneath.

Link each character to their password

Characters

Mario

Iron Man

Frozen

Paul Pogba

Papa Smurf

Cristiano Ronaldo

Ash Ketchum

Aladdin

Shrek

Winnie the Pooh

Available Passwords

Letitgo

Jasmine

Pok151kanto

EuroChampion2016

Muchroomkingdom

Available Passwords

bluemangroup

T.Stark

Honeypots21

AlfinPogform

GreenOgre

Note: **if we come across a list of weak passwords like these, it is relatively easy to guess to whom they belong as well as the meaning contained in the terms**. The programs used to 'crack' password use vast and varied dictionaries – it is always better to invent codes without numerical or literary signification and which will therefore not show up in dictionaries. Make something up yourself!

4 Creating a password using a personal mnemonic

Now that participants have understood what not to do, it's time to give some advice about how to create a password that they won't forget. It would be wise to recall that a 'strong' password must contain at least 8 characters: lower and upper case, numbers and at least one special symbol. **What do we need in a password?** A password must be *long* so that no one can reasonably guess it. It should never be written down, but should be memorised and never be used for more than one account.

***Solution:* Come up with a personal mnemonic that will make it easy for you to retain a complex password that would otherwise be impossible to guess.** Here is how we will proceed:

Proposition	Rule	Example

1st	Your nickname in school/in college; my favourite character etc.	First three letters, one of which capitalised	**Man**
2nd	The number of my parents' address/the number of the building where I work/the date of birth of my favourite animal etc.	Three first numbers	**28 → 028**
3rd	The place you will use the password	First three letters, one of which capitalised	**Library → Lib**
Separator	Character or number between each section	special characters: * or = or etc.	**, then ; then :**
Result		Password for the library	**Man,028;Med:**
Result		Password for work	**Man,028;Ovh:**
Result		Password for school	**Man,028;Ana:**
Optional	Your password must change at set intervals	Change your password for second semester of 2020	**Man,028;Med:1T19!** **Man,028;Ovh:1T19!** **Man,028;Ana:1T19!**

5 Application

For those with a library card, we propose you replace your account password with their own based on what you have learned here. This can obviously be done with at any other access point or website requiring a password. Effectively, everything we've just learned to create a secure password can be used to invent passwords for websites.

6 Mnemonic instructions for complex passwords

Remember:

- Your password should be composed of around 13 characters.
- Your password should be composed of 3 parts, each of different types of characters (numbers and lower case letters). One of the parts should be based on a place (the site for which you created the site), and each part should be separated by a punctuation mark of your choice.
- You should avoid combinations of letters such as those found in your name, the city where you were born or where you live currently as well as numbers contained in your date of birth or current or past postal codes.
- The more different types of characters there are, the more difficult it is the crack a password: use numbers, letters (lower and upper case) and special characters such as * or = or + or, etc.
- The more often we change a password for an account, the more difficult it will be for a hacker or program to crack the code. You should therefore decide to change yours at set intervals.
- Each password should be used for only one account. Otherwise, if your password is discovered for one of your accounts, a would-be perpetrator could quickly and easily access all your other accounts.
- Never leave a written trace of your secret code: the less it’s written and the less it’s uttered aloud, the easier it will be to keep it secret. The ideal password is located only in our heads.

7 Going further

https://arstechnica.com/information-technology/2013/05/how-crackers-make-minced-meat-out-of-your-passwords/ https://xkcd.com/936/