TOOL – PASSWORDS

SAFETY > 4.1 PROTECTING DEVICES

TARGET GROUP	AGE GROUP	PROFICIENCY LEVEL	FORMAT	COPYRIGHT	LANGUAGE
Facilitators	N/A	Level 1	Preparatory guide	Creative Commons (BY-SA)	English, French

This document contains background information for facilitators before they run the workshop with participants. It helps to understand the importance of possessing strong passwords and how to create them by using online tools.

General Objective	Knowledge acquisition
Preparation time for facilitator	less than 1 hour
Competence area	4 - Safety
Name of author	Samantha Giordano
Resource originally created in	French

WORKSHOP DIRECTIONS

1 What's a password?

A password is a method of authentication which allows us to prove our identities on various platforms (email accounts, banking apps, social networks, etc…). Passwords help us to protect our personal information. We choose a password when we create our account. It should be unique and should remain secret – we must never reveal it!

It is therefore a crucial part of our digital identity. If our passwords are badly managed, it can be catastrophic both for our private and financial lives, leaving us at the mercy of cybercriminals. Choose a strong password as therefore essentially and deserves some thought.

For some information on the history of passwords, see this Wikipedia article.

2 How to create a strong password

To secure your personal data, it is recommended to use strong passwords that are different for each application and renewed regularly.

A strong password should contain:

- at least 8 characters
- a mix of character types, e.g. lowercase and uppercase letters as well as special characters ($, @; #, etc.)
- should be totally abstract, containing no links to your personal life

To verify the strength of your password, test it by using howsecureismypassword.net.

Be aware that there are many password testers, many of which exist to add your password to a database to later conduct password dictionary attacks. You should only use password tester from organisations or sites you trust.

In case of doubt, replace your password's characters with the adjacent letter alphabetically or the following or preceding number.

Realise that the world's most used password is '123456'.

There are several techniques for creating a password. Here is very simple one:

- choose 2 words of no relationship
- capitalise the first letter
- Insert a special character between the two words
- Add a number at the end

The ideal would be to have a different password for every site. To avoid having to memorise too many, you can keep the same password but add the first letters of the site for which you create an account for example.

3 Password managers

If you use many passwords and fear losing them, there are free password managers that will memorise them for you.

For this, you will need to download the program and create a 'master password' which will allow you to access the program and thus your other passwords. In this case you only need to memorise one password. Make sure this one is strong!

Here are some examples:

- Bitwarden (see a workshop tool on the subject here)
- Dashlane
- KeePass

4 Going further

See this article for some further tips on creating strong passwords.

See our information sheet 'Hacking and Cybercrime' for more information on how secure your personal

data.