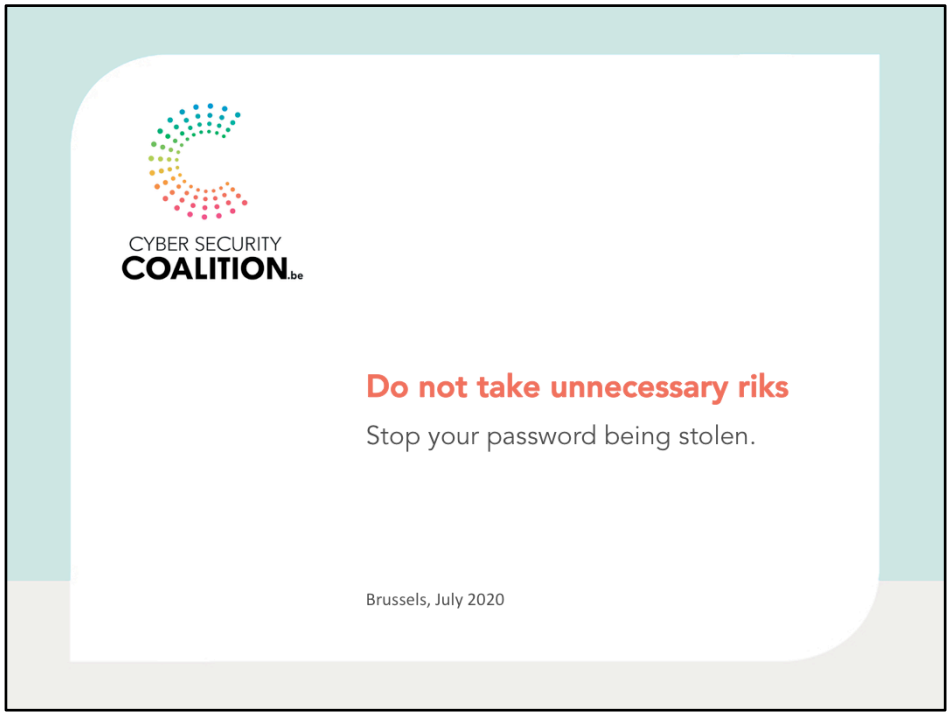
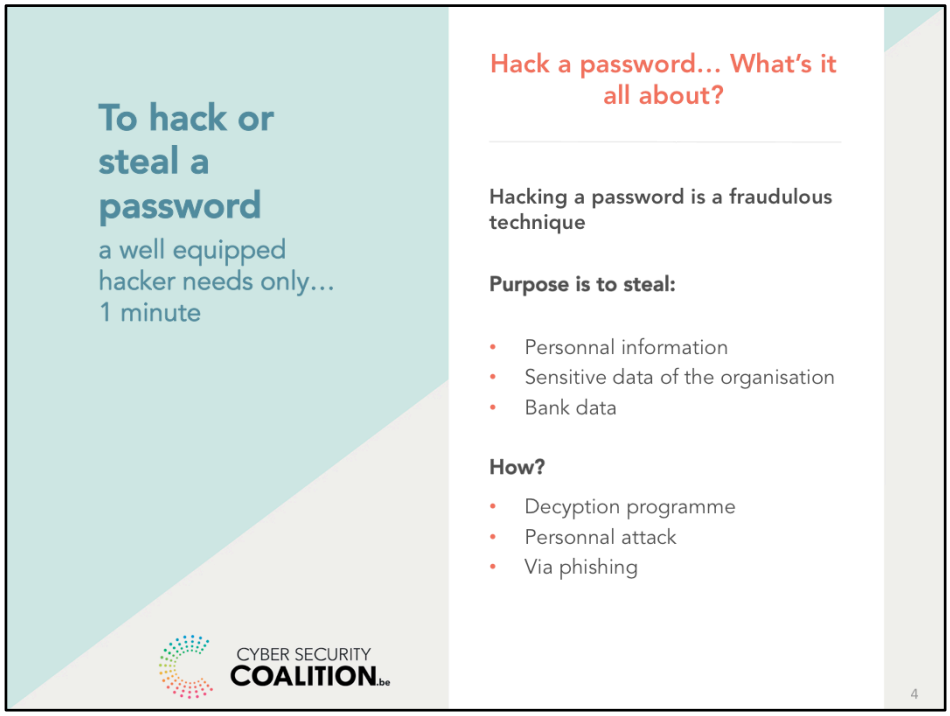


Hello and welcome everyone!

A classic hacking scenario with SME.

Attention: hacking!
A person with bad intentions **hacked your password**. In fact this person has your keys in his hands. He can steal **confidential information**, send messages on your behalf to **all your contacts** (friends, colleagues, clients). He can log in in **social networks** with your profile and buy stuff on your favourite sites.



Hacking passwords is a fraudulous technique which consists of **stealing a password to get access to professional and personal accounts**.

The purpose?
- Looking for **personal information** (ID, passswords, credit card number).
- Access to **sensitive data** in your organisation.
- **Steal money** by getting access to your bank data.

How?
- Hacker uses **decryption program** for passwords.
- Een personal attack, an acquaintance or a third who has direct access to your password.
- A **phishing e-mail** which gave access to your data in a fraudulous way.

Almost half of the Belgians use a weak password with **less than 8 characters**.

Disturbing! **1 Belgian on 3 shares his password** with a third, someone he knows or not.

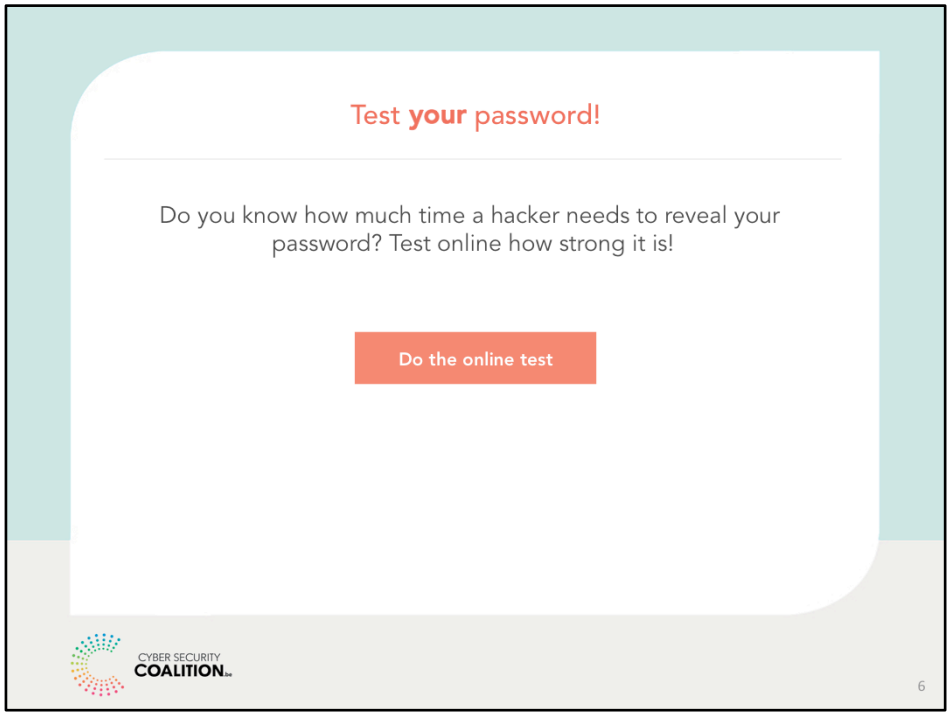
Another alarming number for SME: **1 Belgian on 4 uses the same password for professional and personal reasons**.

15% of Belgians use **only 1 password**. (Safeonweb, Digital Health Index 2018)

Keeping track of passwords can be tricky. Use an online password manager. Various kinds are available, both free and at a price. **Only 16% of Belgians use a password manager**. (Safeonweb, Digital Health Index 2018). Password managers remember all of your passwords. It is best to secure them with a strong password - so you only have to remember one.

39% of Belgians occasionally or frequently use 2FA (2 Factor Authentication, see slide 8). (Safeonweb, Digital Health Index 2018).

123456, qwerty, Star Wars or name and year of birth (like YourName 1985) are the most common passwords. This is a bad idea: there are programmes that can crack these kinds of passwords automatically, or try any and every combination of characters almost instantly.



Test on: https://www.grc.com/haystack.htm

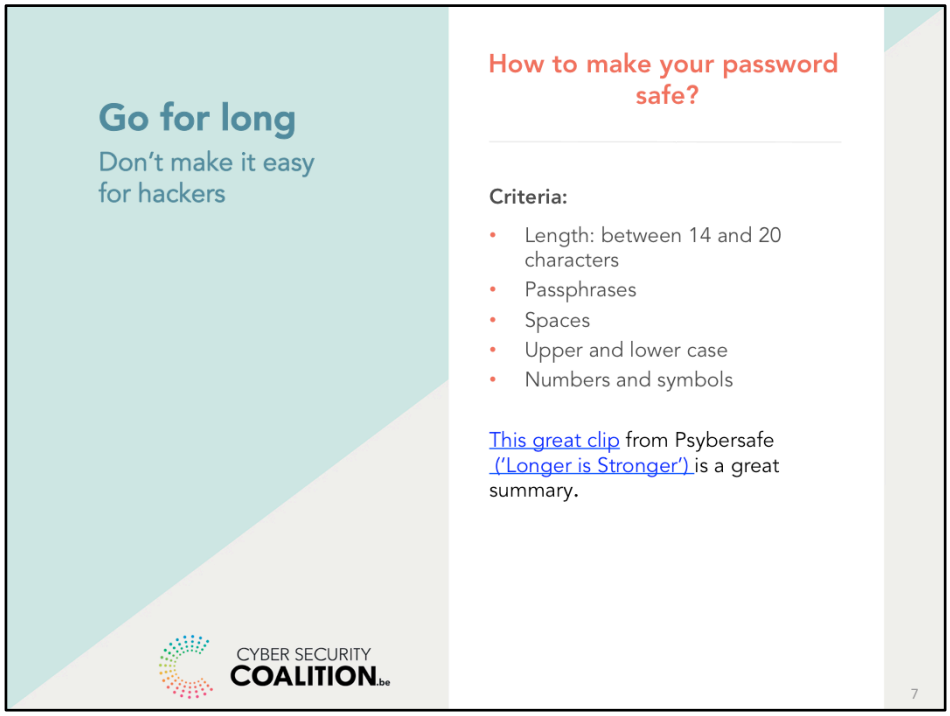
In this **anonymous test** you don't have to introduce your password of course!

You answer a few questions; then you'll know how much time a hacker needs to reveal your passsword.

- And how fast?
- Challenge your colleagues: who has the most complicated password?

May be less strong than you thought. But no panic… you have time to change it …now.

And of course you should NEVER tell someone else your password.



Strengthen your password

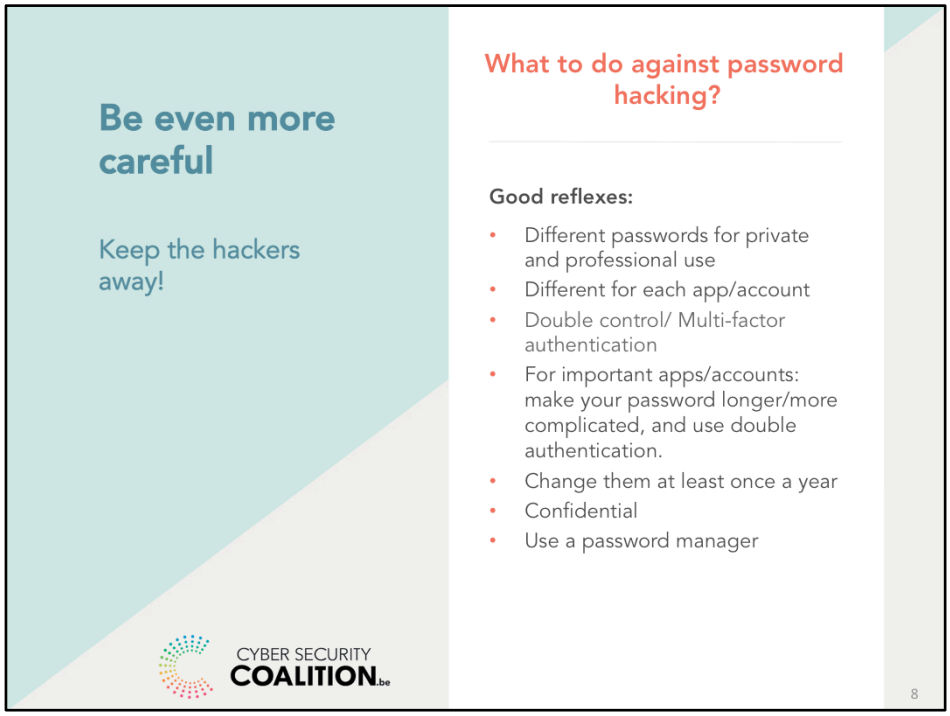
- Make it longer, between **14 and 20 characters**.
- Choose **passphrases**, easy to remember and difficult to guess.
- Keep the **spaces**, easy to type.
- Use **upper and lower case**.
- Add **numbers and symbols**.

Strong doesn't mean complicated

There's a common myth that strong passwords have to be as complicated as possible, but passwords like these are difficult to remember, tricky to type, and cyberattackers can use modern super-fast computers to crack them easily. The key to passwords making them **long**: **the more characters the better**. We call these passphrases: very strong passwords that are actually short sentences, or simply random words, like 'ineedsomemorecoffee!' or 'fast-slug-crawling - sandpit'. Both of these are over 12 characters long, they're easy to remember, and easy to type - but hard to crack!
If the system requires your password to contain symbols, digits, or capital letters, they can be added easily.

If you can't use at least 14 characters, continue to use the 'old' standard of at least one capital letter, one lower-case letter, a digit, and a special character.
Unfortunately, the most common passwords continue to be: 123456, 123456789, qwerty, password or 11111 (UK Cybersurvey, 2019).

This great clip from Psybersafe ('Longer is Stronger') is a great summary:
https://vimeo.com/426500246/a76c9905ab



Take good reflexes against hacking

- Choose **different passwords for professional and private use**.
- Prefer a **double control**, via e.g. an SMS-code.
- **Don't save you password in your browser**.
- **Don't pass** along your password to **other people**.
- **Use different passwords for each app/account.**Cybercriminals often try stolen passwords on as many different Internet services as they can. This way, if criminals get their hands on your password for one service, they won't automatically be able to access your other accounts.
- **Where possible, use double authentication** like a password combined with an SMS code (this is known as **2 Factor Authentication or Multi-Factor Authentication**, see below).
- For important apps/accounts: make your password longer/more complicated, and use double authentication (2FA).
- Change your password at least once a year. Do not use old passwords or parts of them. For example, don't change 'Ahorseanditsjocky2016' to 'Ahorseanditsjockey2017'.
- **Don't pass** along your password to **other people**.
- Use a **password manager**: an app which manages all your passwords (you have to memorize only one password, the one that gives access to your passwordmanager); e.g. LastPass, OnePass, Dashlane, Keepass

Source: Vrije Universiteit Brussel

Multi-Factor Authentication (MFA) is an authentication method that requires the user to successfully complete at least two steps (factors) to gain access to something.

Typical factors:
1. Something you know (most people know about this factor): username and password.
2. Something you are: this includes all biometric data like fingerprints, facial recognition and iris scans.
3. Something you have: common examples of this factor are key cards and hardware tokens. The device the user is operating on can also be used as a factor, only allowing access from a 'trusted device'.
4. Location: this factor requires the user to be in a given location to gain access. This can be a geographical or a network limitation.
Step one: user enters username and password. Step two: user must perform another action. This can be entering a second key such as a code sent by text message or a code received from or created by a linked app on the user's smartphone, or simply confirming the login request on such an app. This is a typical example of two-factor authentication (2FA).

Why Multi-Factor Authentication?
Antivirus, firewalls, encryption, and other information security measures are not effective if cybercriminals are able to pose as legitimate users. If a cybercriminal uses your compromised login information to sign in, the system will think you logged in and let the cybercriminal do everything you're authorised to do.

MFA improves login data security, and has become a crucial part of information security. If your password is compromised, cybercriminals cannot use your password on its own as the 2nd factor is still needed.

It is also closer to compliance with the law. The General Data Protection Regulation (GDPR) requires sensitive personal data protection to be optimised. MFA is a significant step towards achieving this.

Limits of Multi-Factor Authentication.
MFA is not a silver bullet against cyber criminals. It doesn't stop users from falling for attempts at phishing, with an unsuspecting user being directed to a fake website and logging in using MFA. This means the cybercriminal has obtained both factors and can use them to log in once themselves. Text messages containing the 2nd factor can also be intercepted by a process called SIM cloning, with criminals making a duplicate of your phone which receives copies of all your text messages.

Despite these limitations, though, MFA is still the simplest protection against compromised passwords being misused, and it is highly efficient. MFA is increasingly seen as the minimum security authentication.

How to react when your password has been hacked?

- Alarm the **responsible** in your organisation.
- **Contact the service** that manages the hacked account.
- **Warn** your contacts via another chanel.
- Change all your **passwords** and make them stronger (=longer): change your password if someone has, or might have, accessed your account, e.g. if someone tells you they got strange messages from your account. You should also change your password if the service with which you have an account is involved in a data breach. This will prevent people who accessed this service from abusing your account information. You can check whether your e-mail address is listed in a leaked database on the website www.haveibeenpwned.com.
- Run an **antivirus control** on your computer.

What is your opinion?
Do you have remarks?
What do you remember?
What will be your first action after this presentation?

Thank you for your attention!