3/ Passwords and Account Protection

Things to consider

- The techniques and software used to break passwords have evolved significantly over the past few years. It takes more effort to make strong passwords now.
- Brute-force dictionary attacks are used to guess passwords, which can now also decipher patterns with numbers and symbols.
- A number of servers of online service providers have been compromised in recent years. This has led to the leaking of a huge number of passwords onto the open internet. Brute force attacks may also include these stolen passwords.

Protection tactics

- Passwords should not be easy to guess, and should be **long** (12-15 characters minimum), including numbers, letters, and symbols. They should also be **changed regularly**.
- Avoid using the **same password** for more than one account.
- **Use passphrases** rather than passwords: phrases consisting of several words, ideally unrelated, and also including symbols and numbers. This is much more difficult for dictionary-based password-cracking software to guess.
- **Don't trust your browser** to save passwords. The underpinning security of these services is often undocumented.
- **Use a password management software** to generate stronger passwords and passphrases. These tools can also save your passwords using a "master password", so that you do not need to remember them. Choose one with the following characteristics:
  - **Open-source:** given that the software is managing the keys to your sensitive data, it should be open source and/or subjected to independent audits to verify its security bona fides.
  - **Strong encryption:** the software should use strong encryption to store your passwords securely.
- **Use two-factor authentication (2FA):** After entering your password to log in, you will be asked for a further code which is often generated in an app or sent to your phone via a messaging service.
- **Be smarter with "secret questions":** These are questions relating to your personal life and can easily be guessed. Generate random or long passphrases as "answers" to these questions, and save them in your password manager.
- Frequently check if your email addresses have been included in recent **data breaches**, through services such as the "Have I been Pwned" website or the database provided by the Hasso Plattner Institute.