HOW TO CREATE A SECURE PASSWORD THAT IS EASY TO REMEMBER?

Practical guide for end users and non-technical users

A good password should be:
long, unique, hard to guess, and easy for you to remember.

STEP BY STEP

1. Think of a phrase you can remember
Choose a simple and personal phrase that means something to you.
Example: "My coffee makes me happy every morning".

2. Turn the phrase into a base
You can join words, use initials, or use a mix that is easy to remember. Example: "MyCoffeeMakesMeHappyEveryMorning".

3. Make it longer
The longer it is, the better. Try to make it at least 14 characters long.

4. Add uppercase letters, numbers, and symbols
Add one or two elements that are easy for you to remember.
Example: "MyCoffeeMakesMeHappyEveryMorning!27".

5. Use a personal rule
You can repeat a pattern that only you understand, for example: always add a symbol at the end and two numbers you remember.

6. Do not use obvious data
Avoid your name, date of birth, 123456, qwerty or information that is easy to guess.

7. Use a different password for each important account
Email, banking, and social media should have different passwords. If you can, use a password manager.

Personal phrase + Length + Aa + 12 + Symbol

ILLUSTRATIVE EXAMPLE:

MyCoffeeMakesMeHappyEveryMorning!27

FINAL CHECKLIST

- It has 14 characters or more
- It combines letters, numbers, and symbols
- It does not use obvious data
- It is easy for me to remember
- I do not reuse it for all my accounts
- I store it securely

AVOID THIS

- 123456 or password
- Your name + date of birth
- The same password for everything
- Words that are too simple
- Sharing it by message or on visible paper

EXTRA TIP

If an account is important, also enable **2-step verification.**