### TASK 6: CREATING A STRONG PASSWORD AND EVALUATING ITS STRENGTH.

STEP 1: try random passwords to check the strength of the password

STEP 2: usage of online free tool to analyze the password(eg: passwordmonster)

- Use random password of your choice to evaluate the strength of passwords
- Example: use passwords with characters, symbols, different lengths, numbers etc

PasswordMonster info@passwordmonster.com

# **How Secure is Your Password?**

Take the Passwor Tip:	u iesi		Sh	ow password: 🔽
	Passv	word		
	Very V	Veak		
8 characters containing:	Lower case	Upper case	Numbers	Symbols
	Time to crack yo			
Review: Oh dear, using that part very v	ssword is like leav veak because it is	• ,		ır password is
Your passwords are nev	er stored. Even if 1	they were, we hav	e no idea who yo	u are!

PasswordMonster info@passwordmonster.com

## **How Secure is Your Password?**

#### Take the Password Test

**Tip:** It's often better to have longer passwords than shorter, more complex ones

990011223344

Medium

12 characters containing: Lower case Upper case Numbers Symbols

Show password:

Time to crack your password: 4 hours

Review: Hmm, using that password is like locking your front door, but leaving the key under the mat.

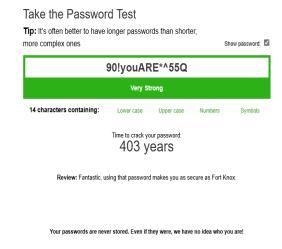
Your password is of medium strength because it contains a dictionary word and a common password.

Your passwords are never stored. Even if they were, we have no idea who you are!









In the above example I have used mixture of characters, symbols and numbers to make a password strong

### STEP 4: Evaluate your passwords

• The password must:

Be long – Aim for at least 12 to 16 characters.

- •Including a mix of characters Use uppercase and lowercase letters, numbers, and special characters.
- •Avoiding common words or phrases Words like "password" or "123456" are easily guessed.
- •Being unique Never reuse passwords across multiple accounts.

## **How Does Complexity Affect Security?**

•Longer passwords take exponentially longer to crack.

A **6-character password** can be cracked in **seconds**, while a **16-character password** could take **75 years**.

- •Using phrases or sentences makes passwords harder to guess.
- For example: ("HotChocolateOnRa1nyDays!" would take **centuries** to crack).
- •Adding (random characters) increases security. For example, "" would take **centuries** to crack.

## **Best Tips for Creating Secure Passwords**

**Use passphrases** – A sentence like "I love to eat pizza every Friday night!" can be turned into "Il2ep3Fn!".

**Usage of password generators** – Random password generators create complex, unique passwords.

Use a password manager – Helps store and manage passwords securely. Enable multi-factor authentication (MFA) – Adds an extra layer of security.