Create a Strong Password and Evaluate Its Strength

1. Create multiple passwords with varying complexity

Create **at least 6–8 passwords** across different complexity levels:

Type	**Password Example**	**Characteristics**
Weak	password	All lowercase, common word
Medium	Password123	Capital letter, numbers
Medium-Strong	MyDog2024	Mix of cases and numbers
Strong	P@ssw0rd2024!	Mix of symbols, cases, numbers
Stronger	@V!kY_Cyber#2025	Personalized, complex
Very Strong	Pa55w0rd	Random, long, complex

2. Use Uppercase, Lowercase, Numbers, Symbols, and Length Variations

Ensure each password has different combinations:

- **Uppercase**: A-Z
- **Lowercase**: a-z
- **Numbers**: 0-9
- **Symbols**: ! @ # $ % & *
- **Length**: Try passwords with 6, 8, 12, 16+ characters

3. Test Each Password on Password Strength Checker

Go to any of the password strength checker websites and input your passwords one by one.

For each password:

- Record the **score**
- Note **feedback**

4. Note Scores and Feedback from the Tool

Create a table like this:

Password	**Score**	**Time to Crack**	**Feedback**
password	Weak	Instant	Too common
MyDog2024	Medium	5 minutes	Add symbols
P@ssw0rd2024!	Strong	3 years	Good complexity

5. Identify Best Practices for Creating Strong Passwords

From the results, summarize best practices:

- Use at least **12 characters**
- Include a mix of **uppercase, lowercase, numbers, and symbols**
- Avoid using **common words** or **personal info** (e.g., name, birthdate)
- Use **passphrases**
- Do not reuse passwords across accounts

6. Write Down Tips Learned from the Evaluation

Tips you may note:

- A longer password = stronger security
- Random character usage increases cracking time
- Adding symbols and avoiding dictionary words improves strength
- Password managers can help generate and store complex passwords

7. Research Common Password Attacks

Attack Type	Description
Brute Force	Attacker tries **all possible combinations** until the correct one is found.
Dictionary Attack	Uses a list of **common passwords and words** to guess quickly.
Credential Stuffing	Reuses leaked passwords from other sites.
Phishing	Tricks users into **revealing passwords** via fake emails or sites.
Keylogging	Records what a user types to steal passwords.

https://www.security.org/how-secure-is-my-password/

I am check all password in above site strongness of password

1.pa55w0rd is very strong password never cracked one.

2.Vicky@123 its take 3 week to computer the password.

3.