Create a Strong Password and Evaluate Its Strength

Password Strength Evaluation Report:

1.Password created and tested:-

Hello@1984	Uppercase with symbol and dob
Rahul@24_	Uppercase + symbol + numbers
rocky123	Lowercase and short
helloworld	Lowercase, easy and common
Ram.@1357	Uppercase + random number pattern

2.Password Strength Test:-

Tools used to check password strength

I. Password Meter - Gives a percentage score and detailed feedback (length, variety, character types).
II. Haveibeenpwned – Verify that the passwords has been appeared in any real data breaches.

3.Best practices to create strong passwords:-

- Use at least **12–16 characters** in length.
- Mix **uppercase, lowercase, numbers, and symbols**.
- Avoid dictionary words or predictable patterns (e.g:password123).
- Randomness increases resistance to brute force and dictionary attacks
- Use **passphrases** combining random words with symbols/numbers.

4.Result of the passwords:-

s.no	Password	Strength/ Score	Feedback	Pwned Password Result
1	Hello@1984	Very Strong 96%	Upper/Lower,symbol but common pattern and predicable numbers.	Found in data breaches.
2	Rahul@24_	Very Strong 84%	Upper/lower, symbol but personal name and number.	Not found in data breaches.
3	rocky123	Weak 39%	No uppercase,no symbol and continue number which is vulnerable to attacks.	Heavily found in data breaches.
4	helloworld	Very Weak 11%	No uppercase and symbols and short single common phrase.	Heavily found in data breaches.
5	Ram.@1357	Very Strong 100%	Random numbers used and mix of symbols and punctuations .	Not found in data breaches.

5.Common password attacks:-

Attack Type	What it means	Example / How it works	How to stay safe
Brute Force	Tries every possible password until it works.	Tests all combinations like aaaaaa → zzzzzz.	Use long passwords (12+ chars) and enable MFA.
Dictionary Attack	Tries common words or passwords from a list.	password123, hello2025!.	Avoid common words; use unique passphrases.
Hybrid Attack	Combines words with numbers or symbols.	Rocky@123, Admin!2024.	Avoid predictable patterns; use random characters.
Credential Stuffing	Uses leaked passwords from other sites.	Reusing email+password on multiple sites.	Use different passwords per site; use a password manager.
Phishing	Tricks people into giving their password.	Fake email asking you to “log in.”	Don’t click unknown links; enable MFA; never share passwords.