Password Strength Evaluation Table

Password Tested	Score	Complexity	Observations
123456	4%	Very Weak	Common numeric password; too short; no character use; easily guessable using brute force.
qwerty	8%	Very Weak	Common keyboard pattern; short and predictable; no variation in characters.
thisisalongpassword	20%	Weak	Long but lacks uppercase letters, numbers, or symbols; dictionary words.
MyNewPassword	50%	Good	Has uppercase and lowercase letters; lacks numbers and symbols
MyNewPassword123	100%	Very Strong	Good length; includes uppercase, lowercase, and numbers; no symbols.
MyN@wP&ssw0rd!2025	100%	Very Strong	Super Strong use of mixed characters- uppercase, lowercase, symbols, and numbers.
IloveEatingMangoesInSummer!	100%	Very Strong	Long passphrase; good complexity; includes uppercase and symbol; no numbers; secure.

☑ Rules for Creating Strong Passwords

1. **Use at least 12 characters (preferably more)**

- Longer passwords take exponentially more time to crack.
- Short passwords can be broken in seconds by brute force.

2. **Include a mix of character types**

- Uppercase letters (A–Z)
- Lowercase letters (a–z)
- Numbers (0–9)
- Symbols (!, @, #, $, %, etc.)

→ This increases complexity and resists brute force and dictionary attacks.

3. **Avoid using dictionary words or common patterns**

- Passwords like qwerty, password123, or iloveyou are found in most password dictionaries.
- Combine unrelated words or use a passphrase with symbols and numbers.

4. **Don't reuse passwords across accounts**

- If one site is breached, all your accounts become vulnerable.

5. **Avoid personal information**

- Don't use names, birthdays, mobile numbers, or anything guessable.

6. **Use unpredictable combinations**

- Randomness matters. `MyN@wP&ssw0rd!2025` is far stronger than `MyPassword123`.

7. **Consider using passphrases**

- Example: `YellowTiger@Sky2024!` – easy to remember, hard to guess.

8. **Use a password manager**

- They help generate and store strong passwords without you needing to memorize them all

Brute Force Attack :- Brute force attacks operate by generating and checking credentials at high speed. Attackers might start with obvious guesses (e.g., "password" or "123456") and then progress to systematically generating all possible combinations of characters until they discover the correct password. Modern attackers use significant computing power, from multi-core CPUs to cloud computing clusters, to accelerate this process.
For example, a six-character password using only lowercase letters has 26^6 possible combinations, which can be guessed almost instantly with today's hardware. In contrast, a longer password with mixed cases, numbers, and special characters exponentially increases the number of possibilities, making it much harder to crack

The more complex a password is, the **more time and guesses** an attacker needs to crack it.

Password Complexity Includes:

1. **Length** – More characters = more combinations.
2. **Character types** – Using **uppercase, lowercase, numbers, and symbols** increases total possibilities.

Dictionary Attacks :- A Dictionary attack is a method used by hackers to guess password by trying words from a predefined list of common passwords or dictionary words.A dictionary attack is based on trying all the strings in a pre-arranged listing. Such attacks originally used words found in a dictionary (hence the phrase *dictionary attack*); however, now there are much larger lists available on the open Internet containing hundreds of millions of passwords recovered from past data breaches. There is also cracking software that can use such lists and produce common variations, such as substituting numbers for similar-looking letters. A dictionary attack tries only those possibilities which are deemed most likely to succeed. Dictionary attacks often succeed because many people have a tendency to choose short passwords that are ordinary words or common passwords; or variants obtained, for example, by appending a digit or punctuation character. Dictionary attacks are often successful, since many commonly used password creation techniques are covered by the available lists, combined with cracking software pattern generation. A safer approach is to randomly generate a long password (15 letters or more) or a multiword passphrase, using a password manager program or manually typing a password.

A complex password is **not likely to be in any dictionary** or common-password list.

Defenses:

1. **Uncommon combinations** – Complex passwords use random characters, not predictable words.
2. **Length** – Longer passwords are unlikely to match dictionary entries.
3. **Symbols & Numbers** – Adding `@`, `!`, or `123` makes the password unpredictable.