Task 6 : Create a Strong Password and Evaluate Its Strength.

Project: Evaluating strong password
Author: Damini S
Date: 30-09-2025
Tool Used: passwordmeter.com

Objective

To understand what makes a password strong, test different passwords using online password strength checkers (e.g., passwordmeter.com), and analyse the results.

1. Passwords Created

I generated passwords with different levels of complexity:

1. apple123
2. Cat2025
3. @pple2025
4. D@m!n!2025
5. #Xy!8pLq9@Tz$7

2. Password Strength Testing Results

Password	Length	Complexity	Strength Score (PasswordMeter)	Feedback
apple123	9	lowercase + numbers	Weak (37%)	Too short, predictable, dictionary word, lacks symbols/uppercase.
Cat2025	7	Uppercase + lowercase + numbers	Fair (47%)	Still predictable, no symbols, moderate length.
@pple2025	9	Mixed case + numbers + symbols	Strong (68%)	Improved with symbols, but still close to dictionary word "apple".
d@m!n!01	7	Upper/lower + numbers + symbols	Very Strong (81%)	Good entropy, difficult to guess, long enough.

Password	Length	Complexity	Strength Score (PasswordMeter)	Feedback
#Xy!8pLq9@Tz$7	14	Random mix of all character sets	Excellent (100%)	High entropy, random, resistant to dictionary/brute force attacks.

3. Best Practices for Strong Passwords

From the evaluation:

- Use **at least 12–14 characters**.
- Mix **uppercase, lowercase, numbers, and special symbols**.
- Avoid dictionary words, names, or personal info.
- Use **random combinations** instead of predictable patterns.
- Store passwords securely using a **password manager**.

4. Tips Learned

- Length > Complexity → Longer random passwords are much harder to crack.
- Substituting symbols for letters (like P@ssw0rd) is not enough if the base word is common.
- Random characters or passphrases drastically increase resistance to attacks.
- Reuse of passwords across sites is highly dangerous.

5. Common Password Attacks

- **Brute Force Attack** – Systematically tries all combinations until the correct password is found. Short/simple passwords fall quickly.
- **Dictionary Attack** – Uses a precompiled list of common words and variations (e.g., password123). Weak if password contains dictionary words.
- **Hybrid Attack** – Combines dictionary + brute force (e.g., trying password@2024).
- **Phishing / Social Engineering** – Attackers trick users into revealing passwords.

6. How Password Complexity Affects Security

- **Short + Simple Passwords** → Easily broken within seconds/minutes by brute force.
- **Longer Passwords with Mixed Characters** → Increases possible combinations exponentially, making brute force infeasible.

- **Truly Random or Passphrases** → Offer the highest protection against dictionary and brute force attacks.