Task 6: Password Strength Evaluation

# Objective

To understand what makes a password strong by creating and evaluating multiple passwords using online password strength-checking tools.

# Tools Used

- PasswordMeter (https://passwordmeter.com)  
- Security.org Password Checker (https://www.security.org/how-secure-is-my-password/)  
- Kaspersky Password Checker (https://www.kaspersky.com/password-check)

# Password Evaluation

## Password: sanika123

Result: Weak

Reason: Contains only lowercase letters and digits. Very predictable and short.

Estimated Crack Time: Less than a second

Feedback: Easily guessable, vulnerable to dictionary and brute force attacks.

## Password: Sanika123

Result: Moderate

Reason: Introduced uppercase letter. Still based on a name and numbers.

Estimated Crack Time: A few seconds to a minute

Feedback: Common pattern, still weak against automated attacks.

## Password: Sanika@123

Result: Strong

Reason: Includes uppercase, lowercase, numbers, and a symbol.

Estimated Crack Time: Several hours

Feedback: Good complexity, but still somewhat predictable structure.

## Password: S@niKa!2025#

Result: Very Strong

Reason: Multiple special characters, mixed casing, non-linear structure, good length.

Estimated Crack Time: Several years

Feedback: High resistance to brute force and dictionary attacks.

# Final Summary

Through this task, I explored how password complexity affects its strength and resistance to attacks. Strong passwords should:  
- Be at least 12–16 characters long  
- Include uppercase and lowercase letters, numbers, and special characters  
- Avoid personal information like names, birthdays, or common phrases  
- Be unpredictable and unique  
  
Using a password manager can help generate and store strong passwords securely. Also, enabling multi-factor authentication (MFA) adds another critical layer of security.