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

## Objective:

Understand what makes a password strong and test it against password strength tools.

## Tools:

passwordmeter.com

## Process / Steps Followed:

1. Created multiple passwords with varying complexity.

2. Used uppercase, lowercase, numbers, symbols, and different lengths.

3. Tested each password on passwordmeter.com.

4. Noted scores and feedback from the tool.

5. Identified best practices for creating strong passwords.

6. Researched common password attacks such as brute force and dictionary attacks.

7. Summarized how password complexity affects security.

## Example Passwords & Strength Evaluation:

|  |  |  |
| --- | --- | --- |
| Password | Strength Score | Feedback |
| password123 | 20% | Weak - common and predictable. |
| P@ssw0rd | 45% | Medium - better complexity but still predictable. |
| G#7tLx!2Qm^B | 95% | Strong - long, random, and complex. |

## Best Practices for Creating Strong Passwords:

• Use at least 12–16 characters.

• Include uppercase, lowercase, numbers, and symbols.

• Avoid common words or predictable patterns.

• Do not reuse passwords across different accounts.

• Use a password manager to store and generate passwords.

## Common Password Attacks:

• Brute Force Attack – trying all possible combinations until the correct one is found.

• Dictionary Attack – using precompiled lists of common words/passwords.

• Phishing – tricking the user into revealing their password.

• Keylogging – recording the keys typed on a keyboard to capture passwords.

## Summary:

Password complexity significantly affects security. Longer passwords with varied character sets are exponentially harder to crack, especially against brute force and dictionary attacks. Following best practices and avoiding common patterns ensures stronger security.