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

## Objective

To create multiple passwords of varying complexity, test them using an online password strength checker, and understand how complexity impacts password security.

## Tools Used

- Website: https://passwordmeter.com  
- Evaluation Criteria: Password length, inclusion of uppercase/lowercase letters, numbers, and special symbols.

## Step-by-Step Process

### 1. Created Multiple Passwords

|  |  |  |
| --- | --- | --- |
| Password Example | Complexity | Length |
| password | Only lowercase letters | 8 |
| Password1 | Uppercase + lowercase + number | 9 |
| Pass@123 | Uppercase + lowercase + number + symbol | 8 |
| P@ssw0rd2025! | Mixed case + numbers + symbols | 13 |
| T!g3r$Tr0nG#2025 | Very complex, random mix | 15 |

### 2. Tested Passwords in PasswordMeter

|  |  |  |
| --- | --- | --- |
| Password | Score (%) | Strength Feedback |
| password | 5% | Too short, common word, no complexity. |
| Password1 | 45% | Better but still predictable; lacks symbol variety. |
| Pass@123 | 60% | Good use of symbol and number but still short. |
| P@ssw0rd2025! | 85% | Strong: good length, mixed symbols, numbers. |
| T!g3r$Tr0nG#2025 | 100% | Very strong: long, unpredictable, mixed case, numbers, symbols. |

### 3. Best Practices for Creating Strong Passwords

- Use minimum 12–16 characters.  
- Combine uppercase, lowercase, numbers, and special characters.  
- Avoid dictionary words or personal info (name, DOB).  
- Use passphrases with substitutions (e.g., B3tter$D@y$Ahead!).  
- Prefer randomly generated passwords from a password manager.  
- Do not reuse passwords across accounts.

### 4. Common Password Attacks

- Brute Force Attack – tries all possible combinations; long & complex passwords resist this.  
- Dictionary Attack – uses lists of common words; unique patterns help avoid this.  
- Credential Stuffing – uses stolen username/password pairs; password uniqueness is key.  
- Phishing – tricks you into giving your password; awareness is the defense.

### 5. How Complexity Affects Security

- Length exponentially increases time required for brute force attacks.  
- Variety of characters expands the possible combinations.  
- Randomness prevents dictionary-based attacks.  
- Unpredictability strengthens resistance.

## Conclusion

The strongest password in this test, 'T!g3r$Tr0nG#2025', scored 100% because it is long, random, and contains diverse characters. Complexity significantly reduces the chances of a successful attack, especially when paired with good security practices like using unique passwords and enabling two-factor authentication.