# Password Strength Evaluation Report

Prepared by : Mohammad Arshan Dafedar

Tools used : passwordmeter.com

## Objective

The objective of this exercise is to understand what makes a password strong, evaluate various passwords using an online password strength checker, and summarize best practices for creating secure passwords.

## Comparative Table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Password | Score | Complexity | Strengths | Weaknesses |
| Cant Skip These | 100% | Very Strong | 17 chars, mixed case, number, high length bonus | Few repeats, consecutive lowercase letters |
| StOp\_ThE\_gEnOcIdE | 100% | Very Strong | 19 chars, strong mix of upper/lower/number, high length | Minor repeat deduction, no symbols |
| ab telegram1 | 37% | Weak | Meets min length, has lowercase + number | No uppercase/symbols, consecutive lowercase, low variety |
| Scoreboard | 33% | Weak | Meets min length, some uppercase | No numbers/symbols, letters only, consecutive lowercase |

## Observations

- Length is a major factor: Passwords above ~15 characters scored very high.  
- Character diversity (uppercase, lowercase, numbers, symbols) greatly increases strength.  
- Passwords with only letters are weak against dictionary attacks.  
- Repeated characters and consecutive lowercase letters reduce the score.  
- At least 3 of the 4 character types with good length is ideal.

## Best Practices for Strong Passwords

1. Aim for 15+ characters — more is better.  
2. Mix character types — include uppercase, lowercase, numbers, and at least one symbol.  
3. Avoid dictionary words or predictable phrases.  
4. Don’t reuse passwords across accounts.  
5. Break up patterns — avoid consecutive letters, numbers, or repeated characters.  
6. Consider using passphrases with random words and symbols.  
7. Use a password manager for unique, complex passwords for every account.

## Common Password Attacks & Why Complexity Matters

Brute Force Attacks: Try all possible combinations. Long, varied passwords make this computationally infeasible.  
Dictionary Attacks: Use lists of common words. Mixing unrelated words with symbols/numbers makes this ineffective.  
Hybrid Attacks: Combine dictionary words with simple substitutions. Complex, random sequences resist these.  
Credential Stuffing: Uses leaked passwords from other breaches. Unique passwords prevent cross-account compromise.  
  
Bottom Line: High length + diverse character types = maximum resistance to cracking methods.