⍰ README – Password Strength Evaluation Task

⍰ Project Title: Password Strength Evaluation

⍰⍰ Prepared by: Suraj Mishra

⍰ Date: 01 July 2025

⍰ Objective:

Understand what makes a password strong and test it against password strength tools to evaluate its security.

⍰ Tools Used:

- ⍰ Website: https://passwordmeter.com

- ⍰ Browser: Chrome or any modern browser

✔Steps Followed:

- • Created multiple passwords with different complexity (length, characters, symbols, numbers).
- • Tested each password on https://passwordmeter.com.
- • Noted down feedback, strength scores, and tool comments.
- • Compared weak vs strong passwords.
- • Learned best practices for creating secure passwords.
- • Researched types of password attacks (Brute Force, Dictionary, Phishing).
- • Wrote a report explaining findings and outcomes.

⍰ Output Files:

- ⍰ Password_Strength_Evaluation_Report_by_Suraj_Mishra.docx – Main report

- ⍰ Screenshots of password tool (optional)

- ⍰ This README file

⍰ Key Learnings:

- ⍰ Passwords must be long (12+ characters).

- □ Include uppercase, lowercase, numbers, and symbols.
- □ Avoid personal info like name or date of birth.
- □ Use password managers and enable 2FA.
- □ Complex passwords are exponentially harder to crack.

□ Common Attacks Studied:

Attack Type	Description
Brute Force	Tries all possible combinations
Dictionary Attack	Uses common passwords/words list
Phishing	Tricks user into giving password

□ How to Use:

- • Open the `.docx` file to read the full report.
- • Visit https://passwordmeter.com to test your own passwords.
- • Use the listed tips to create strong passwords in daily life.

□ Outcome:

This task improved my understanding of digital password security and taught me how complexity directly strengthens online protection.