Task 6: Password Strength Evaluation Report
Date: 01-07-25

Objective:

Evaluate the strength of different passwords using online tools and understand the principles of password security.

Use Online Password Strength Checkers:

Example: https://www.security.org/how-secure-is-my-password/

Here are four passwords of varying strengths,

- sunshine1
- Hello2025
- V@na!47Green
- 9uR!xD&4l#BfPz

Strength	Password	Characteristics
Weak	`sunshine1`	Common word, lowercase + number, short length
Moderate	`Hello2025!`	Upper + lower case, number, symbol, moderate length
Strong	`V@na!47Green`	Mixed case, digits, special characters, 12+ chars
Very Strong	`9uR!xD&4l#BfPz`	14 random characters, high complexity

Lessons Learned:

- Length + complexity = stronger password
- Avoid using predictable patterns or dictionary words
- Use passphrases or random generators
- Always use unique passwords per site

Common Password Attack Methods:

- Brute-force
- Dictionary attacks
- Phishing
- Credential stuffing

Conclusion:

Strong passwords are critical to online security. Use password managers to maintain long, complex, and unique credentials across services.