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 Used

- Online password strength checker: passwordmeter.com

Passwords Tested & Results

Password	Score (%)	Strength Level	Feedback from Tool
apple	12%	Very Weak	Too short, only lowercase letters
Apple123	48%	Weak	Add symbols, increase length
App!e123	62%	Medium	Increase length for better security
App!e12345	74%	Strong	Could add more variety and length
Str0ng!Passw0rd#2025	94%	Very Strong	Excellent length and complexity

---

Observations

- Short passwords are significantly weaker, even with some complexity.
- Adding uppercase, lowercase, numbers, and symbols improves strength.
- Longer passwords with mixed character types provide the best resistance against attacks.

Best Practices for Creating Strong Passwords

1. Use at least **12–16 characters**.
2. Combine **uppercase**, **lowercase**, **numbers**, and **symbols**.
3. Avoid dictionary words and common phrases.

4. Do not reuse passwords for multiple accounts.
5. Use a password manager to generate and store complex passwords.

Tips Learned from Evaluation

- Adding just one symbol or number greatly increases the score.
- Increasing password length by 3–4 characters can raise strength from “Medium” to “Strong”.
- Complex and unique passwords are harder to guess.

Common Password Attacks

- **Brute Force Attack**: Tries every possible character combination until the correct password is found. Longer and more complex passwords make this approach time-consuming.
- **Dictionary Attack**: Uses a precompiled list of common passwords and words to guess quickly. Avoiding dictionary words reduces this risk.

Summary

Password complexity directly impacts security. Strong passwords combine length, variety of characters, and unpredictability, making them resistant to brute force and dictionary attacks. Using these best practices significantly reduces the risk of account compromise.