Password Strength Evaluation Report

Objective: Understand what makes a password strong and test it against password strength tools.

Methodology:

1. Created multiple passwords with varying complexity. 2. Used uppercase, lowercase, numbers, symbols, and length variations. 3. Tested each password on password strength checkers. 4. Noted scores and feedback from the tool. 5. Identified best practices for creating strong passwords. 6. Researched common password attacks. 7. Summarized how password complexity affects security.

Test Results:

Password	Score (%)	Feedback
apple123	34%	Too short, lacks symbols, predictable
Apple2025	54%	Add special characters
ApPLe@2025!	88%	Good strength, could be longer
Gr33n_P@rrot!_42	100%	Excellent
7h!S_I$_V3ry$tr0nG%2025	100%	Very strong, random and long

Best Practices for Strong Passwords:

- Use at least 12–16 characters. - Include uppercase and lowercase letters. - Add numbers and symbols. - Avoid common words or personal information. - Prefer random combinations or passphrases.

Common Password Attacks:

- **Brute Force:** Tries every possible combination. - **Dictionary Attack:** Uses common words/password lists. - **Credential Stuffing:** Uses leaked username/password pairs.

Summary:

Complex passwords significantly increase the difficulty of brute-force and dictionary attacks. Mixing character types, increasing length, and using randomness greatly improve password security.