Password Strength Evaluation Report

Objective:

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

Passwords Tested and Results:

Password	Score	Time to Crack	Feedback
12345678	5%	Instant	Too short, no symbols
Password	10%	Instant	Common word
Pass1234	30%	Few minutes	Predictable pattern
P@ssW0rd!	60%	Few years	Better, but still a known pattern
S!mpl3#Str0ngP@ssw0rd2025	100%	1 trillion years	Excellent

Tips for Creating Strong Passwords:

- Use 12 or more characters.
- Mix uppercase, lowercase, numbers, and symbols.
- Avoid common words and patterns.
- Use passphrases (e.g., L!ghtH0use_@tM1dn1ght).
- Don't reuse old passwords.
- Use a password manager to store passwords securely.

Common Password Attacks:

- Brute Force - tries every possible combination.
- Dictionary Attack - uses common words or phrases.
- Credential Stuffing - reuses stolen passwords from data breaches.
- Phishing - tricks the user into revealing the password via fake messages or websites.

Conclusion:

Password complexity significantly affects security. Strong, unique passwords protect against most common attacks.