Password Strength Evaluation Report

Objective

To understand what makes a password strong and evaluate different passwords using online password strength checkers.

Tools Used

- **passwordmeter.com**

- **howsecureismypassword.net**

1. Passwords Tested

Password	Complexity Details	Score (PasswordMeter)	Time to Crack (HowSecureIsMyPassword)	Feedback
password123	Lowercase, numbers	18%	Instantly	Very weak, common password
P@ssw0rd!	Mixed case, number, symbol	55%	3 hours	Moderate strength, predictable pattern
u&F5w@L9*eR2	Upper, lower, numbers, symbols	88%	45 million years	Strong password
LetMeIn2025	Mixed case, number	36%	2 minutes	Common pattern, weak
3#cV9!qPw7$Lm	Complex mix of all types	96%	Trillions of years	Very strong, random-looking

2. Best Practices for Creating Strong Passwords

- Use a mix of uppercase, lowercase, numbers, and special characters.
- Avoid dictionary words and common phrases.
- Make passwords at least 12 characters long.
- Do not reuse passwords across sites.
- Use a password manager for storing and generating secure passwords.

3. Key Tips Learned

- Password strength significantly increases with randomness and length.
- Predictable substitutions (e.g., '@' for 'a') don't make a weak password strong.
- Tools vary slightly in scoring but agree on core principles.

4. Common Password Attacks

- **Brute Force**: Systematically trying all combinations.
- **Dictionary Attack**: Using a list of known passwords and words.
- **Credential Stuffing**: Reusing passwords from data breaches.

5. Summary

Password complexity directly impacts resistance to attacks. A strong password is long, unpredictable, and uses diverse character types. Using tools helps identify weaknesses and guides users toward safer password practices.