Password Strength Evaluation Report

Objective

To understand what makes a password strong by creating five passwords of varying complexity and testing them with three different online password-strength tools. The goal is to compare password scores, estimated crack times, and feedback and to derive best practices.

Tools Used

- https://passwordmeter.com/ (referred to as PasswordMeter)
- https://www.security.org/... (referred to as Security.org)
- https://bitwarden.com/password-strength/... (referred to as Bitwarden-style tester)

Materials / Evidence

Screenshots:
- Security123: s11.png, s12.png, s13.png
- Secur!ty2025: s21.png, s22.png, s23.png
- MySecureP@ss!: s31.png, s32.png, s33.png
- S#t7!hNpQ2$: s41.png, s42.png, s43.png
- M@rbl3$L!on2025#: s51.png, s52.png, s53.png

Note: filenames correspond to the screenshots in the project folder. Each group contains the three tool outputs for the corresponding password.

Passwords Tested and Results

Password	Password Meter Result	Security.org Crack Time	Bitwarden Tool Result
Security123	77% (Strong)	41 years	10 seconds (Very Weak)
Secur!ty2025	100% (Very Strong)	34,000 years	14 minutes (Very Weak)
MySecureP@ss!	92% (Very Strong)	400,000 years	4 months (Good)
S#t7!hNpQ2$	100% (Excellent)	400,000+ years	4 months (Good)
M@rbl3$L!on2025#	100% (Excellent)	1000+ years	Centuries (Strong)

Important: Different tools use different scoring models and assumptions (e.g., guessed character set, attacker speed, dictionary checks). That explains large differences between tools.

Observations and Analysis

Different tools provide varying strength results. Longer and more random passwords consistently show stronger resistance to brute-force and dictionary attacks. Short, common-word passwords are quickly cracked. Randomness, length, and mixed character sets drastically increase security.

Common Password Attacks

a) Brute-Force Attack:

- Tries every combination of characters until a match is found.
- Cracking time grows exponentially with length and character-set size.

b) Dictionary Attack:

- Uses common passwords and word lists.
- Very effective against human-memorable passwords (dictionary words, common patterns).
- Tools often detect these and drastically reduce the estimated time-to-crack.

c) Credential Stuffing:

- Attackers use stolen username-password pairs from previous breaches.
- Protection: unique passwords per site + 2FA.

d) Hybrid or Mask Attack:

- Combine dictionary words with common digit/symbol permutations (e.g., "Password1!").
- They're faster than pure brute force because they reduce search space cleverly.

Best Practices & Recommendations

- Use a minimum of 12–16 characters.
- Mix **uppercase, lowercase, numbers, and special characters**
- Avoid dictionary words, names, and predictable substitutions (like "P@ssw0rd").
- Use a **password manager** to generate and store complex passwords.
- **Enable Two-Factor Authentication (2FA)** wherever possible.
- Never reuse passwords across multiple accounts.

Effect of Password Complexity on Security

- Increasing complexity and randomness significantly improves resistance to brute-force attacks.
- For example, "password123" can be cracked instantly, whereas "M@rbl3$L!on2025#" may take thousands of years.
- Every additional character increases difficulty exponentially

Tips learned from the evaluation

- Password length matters as much (or more) than complexity.
- Randomness (no words, no sequences) is rewarded by every tool.
- Different checkers will show wildly different crack times, focus on relative improvements rather than a single absolute number.
- Tools like Password Meter are excellent for seeing why a password scores a certain way (they show additions/deductions).

Conclusion

- This task demonstrated that password complexity, randomness, and length directly determine strength and resistance to attacks.
- By testing multiple passwords, it became evident that longer and more complex passwords are significantly more secure.
- Using unique passwords and enabling 2FA are critical steps for maintaining strong account security.