Password Strength Evaluation Report

Tool Used: PasswordMeter.com (Free online password strength checker)

---

1. Passwords Tested

I created multiple passwords with varying complexity to analyze how their structure affects strength:

Password	Length	Complexity	Score (%)	Tool Feedback
sunshine	8	lowercase only	18%	Too short; lacks numbers, symbols, and uppercase letters
Sunshine123	11	uppercase, lowercase, numbers	54%	No symbols; length is fair, but predictable pattern
S#nSh1n3!	9	uppercase, lowercase, numbers, symbols	78%	Strong mix of characters; could be longer for better protection
!Pa55w0rd$2025	14	uppercase, lowercase, numbers, symbols	92%	Very strong; long length and varied character types

Password	Length	Complexity	Score (%)	Tool Feedback
BlueMoon@Sky#2025	17	uppercase, lowercase, numbers, symbols	100%	Excellent; long, complex, and hard to guess

---

2. Best Practices Learned

- **Longer passwords** (12+ characters) drastically improve strength.
- Mixing **uppercase, lowercase, numbers, and symbols** creates more possible combinations.
- Avoid **predictable words** or common sequences (e.g., "1234", "password").
- Adding **random elements** (special characters, mixed case) makes brute-force attacks harder.

---

3. Common Password Attacks

- **Brute Force Attack:** Tries every possible combination until it finds the correct one.
- **Dictionary Attack:** Uses a list of common words and combinations to guess passwords.
- **Credential Stuffing:** Uses stolen usernames and passwords from previous breaches.

---

4. How Complexity Affects Security

Password complexity increases the total number of possible combinations, which **significantly raises the time and computing power needed** for attackers to guess it. For example, an 8-character lowercase password might be cracked in seconds, while a 16-character complex password could take centuries with current computing capabilities.

---

5. Tips for Creating Strong Passwords

1. Use at least **12–16 characters**.
2. Combine **uppercase, lowercase, numbers, and symbols**.
3. Avoid real words, names, and predictable patterns.
4. Consider using a **passphrase** made of unrelated words with special characters (e.g., C@tB3rry!M00n$Star).
5. Use a **password manager** to store complex passwords securely.