Passwords Created for Testing

I created four different passwords with varying lengths and complexity:

1. **sunshine**
2. **Sunshine45**
3. **S!nsh1n3_2025**
4. **M0on!L1ght#Phr@se_9921**

These were entered into PasswordMeter.com, and their scores were recorded.

---

2. Password Strength Evaluation

Password 1: sunshine

- **Strength Score:** 12% (Very Weak)
- **Feedback:**
  - Contains only lowercase letters
  - Too short
  - Dictionary word
  - Easily guessable

Analysis:

This password can be cracked in seconds using dictionary or brute force attacks. It has no complexity and provides minimal security.

Password 2: Sunshine45

- **Strength Score:** 48% (Weak–Moderate)
- **Feedback:**
  - Includes uppercase + lowercase
  - Includes numbers
  - Still based on a dictionary word
  - No symbols

Analysis:

This password is stronger due to added numbers and uppercase letters, but still predictable. Attackers often try combinations like “Sunshine123,” making it risky.

Password 3: S!nsh1n3_2025

- **Strength Score:** 78% (Strong)
- **Feedback:**
  - Good use of uppercase, lowercase, numbers, and symbols
  - Not easily guessable
  - Good length
  - Minor suggestion: increase overall length for maximum strength

Analysis:

The use of symbol substitution (like **!**, **1**, **3**) and the added year makes it significantly harder to crack. Strong protection against dictionary-based attacks.

Password 4: M0on!L1ght#Phr@se_9921

- **Strength Score:** 97% (Very Strong)
- **Feedback:**
  - Excellent length (20+ characters)
  - Complex mix of numbers, symbols, uppercase & lowercase letters
  - Does not resemble any dictionary word
  - Meets all recommended password security standards

Analysis:

This is a very strong password. The length alone makes brute force attacks take centuries. It is random, unpredictable, and follows best practices.

---

3. Best Practices Learned

✓ Use long passwords (16+ characters)

Longer passwords are exponentially more secure.

✓ Combine different character types

- Uppercase
- Lowercase
- Numbers
- Symbols

✓ Avoid dictionary words and predictable patterns

Attackers commonly test simple words and variations (e.g., Sunshine123).

✓ Use passphrases

Example: **Blue!Whale_RunsFast@91**
Easy to remember but extremely hard to crack.

✓ Don’t reuse passwords

Use different passwords for different accounts.

✓ Use a password manager

Helps generate and store strong passwords safely.

---

4. Common Password Attacks (Summary)

Brute Force

- System tries every combination.
- Long, complex passwords resist this.

Dictionary Attack

- Uses lists of common words.
- Avoid real words and predictable patterns.

Credential Stuffing

- Attackers use leaked username/password pairs.
- Unique passwords protect you.

Phishing

- Trick users into entering their password.
- Complexity does NOT protect you—awareness does.

---

5. Final Summary

After testing four passwords of varying complexity, it is clear that **longer passwords with mixed character types are significantly stronger**.
Simple or dictionary-based passwords can be cracked in seconds, while long, complex passphrases can take thousands of years to break.