**Password Strength Evaluation**

**Objective**

To understand the elements that contribute to a strong password and evaluate password strength using free online tools.

**1. Password Creation**

| **Password** | **Uppercase** | **Lowercase** | **Numbers** | **Symbols** | **Length** |
| --- | --- | --- | --- | --- | --- |
| Pass123 | ✅ | ✅ | ✅ | ❌ | 7 |
| P@ssw0rd2025 | ✅ | ✅ | ✅ | ✅ | 12 |
| abcdefg | ❌ | ✅ | ❌ | ❌ | 7 |
| R!$h@bH\_123 | ✅ | ✅ | ✅ | ✅ | 11 |
| A1b2C3 | ✅ | ✅ | ✅ | ❌ | 6 |

**2. Password Strength Evaluation**

*Test Tool Used:* [*https://passwordmeter.com*](https://passwordmeter.com)

| **Password** | **Score (%)** | **Feedback/Suggestions** |
| --- | --- | --- |
| Pass123 | 38% | Too short, lacks symbols |
| P@ssw0rd2025 | 86% | Strong, good use of complexity |
| abcdefg | 14% | Very weak – too simple, too short |
| R!$h@bH\_123 | 92% | Very strong, excellent complexity |
| A1b2C3 | 45% | Moderate – could be longer with symbols |

### ****3. Tips Learned for Strong Passwords****

* Use a mix of **uppercase, lowercase, numbers, and symbols**.
* **Longer passwords** (12+ characters) are stronger.
* Avoid common patterns like “123”, “password”, “abcdef”.
* Do not reuse passwords across multiple accounts.
* Use **passphrases** that are long but memorable (e.g., “Sunset!On@Beach2024”).

### ****4. Common Password Attacks****

* **Brute Force Attack**: Tries every possible combination until the correct one is found. Time-consuming for strong, long passwords.
* **Dictionary Attack**: Uses a list of common words and phrases to guess passwords.
* **Credential Stuffing**: Uses stolen username/password combinations from previous breaches.
* **Phishing**: Trick users into giving passwords away.

### ****5. Summary: How Password Complexity Affects Security****

The complexity of a password significantly increases its resistance to attacks. A simple password like "abcdefg" can be cracked in seconds using a dictionary attack, while a complex one like “R!$h@bH\_123” may take years even with advanced tools. Passwords that use a mix of characters and are sufficiently long are far more secure. Using password managers can help generate and store strong passwords easily.