## **🔐 Password Strength Evaluation Report**

**Internship Task 06** **Name:** Abhishek  
 **Role:** Cybersecurity Intern  
 **Date:** July 2025

### **🎯 Objective:**

To understand what makes a password strong by creating and testing multiple passwords using online tools, and analyzing the results to learn password best practices and security insights.

### **🛠 Tools Used:**

* [PasswordMeter.com](https://www.passwordmeter.com/)
* Security.org Password Checker

### **🔎 Step 1: Password Creation**

Created 5 passwords with different complexity levels:

| **Password** | **Complexity Level** | **Composition** |
| --- | --- | --- |
| abhishek123 | Weak | Lowercase + numbers only |
| Abhishek@123 | Medium | Upper + lower + number + symbol |
| Abhi@2025! | Strong | Good mix + symbolic + current year context |
| aB#98xL!pQ | Very Strong | Random + 10 chars + all elements used |
| password | Very Weak | Common dictionary word |

### **📊 Step 2: Test Results**

**Results from PasswordMeter and Security.org tools:**

| **Password** | **PasswordMeter Score** | **Crack Time Estimate (Security.org)** | **Tool Feedback** |
| --- | --- | --- | --- |
| abhishek123 | 34% (Weak) | Instantly crackable | No uppercase/symbols |
| Abhishek@123 | 86% (Strong) | ~5 years | Good symbol use |
| Abhi@2025! | 92% (Strong) | ~25 years | Effective structure |
| aB#98xL!pQ | 100% (Very Strong) | ~200+ years | Excellent randomness and mix |
| password | 10% (Very Weak) | Instantly crackable | Very common word |

*Screenshots of the tools are saved in the screenshots/ folder of the GitHub repo.*

### **✅ Lessons Learned**

#### **What Makes a Strong Password:**

* At least 10–12 characters
* Mix of:  
  + ✅ Uppercase and lowercase letters
  + ✅ Numbers
  + ✅ Special characters (@, #, $, %, etc.)
* Avoid common names, patterns, or dictionary words
* Use random strings or passphrases
* Change passwords regularly
* Use a password manager

### **🛡️ Research: Common Password Attacks**

| **Attack Type** | **Description** |
| --- | --- |
| Brute Force | Tries every possible character combination |
| Dictionary Attack | Uses common passwords and dictionary words |
| Credential Stuffing | Uses stolen credentials from previous breaches |
| Phishing | Tricks users into providing passwords voluntarily |

### **🔐 Password Complexity & Security**

| **Password Length/Strength** | **Estimated Crack Time** |
| --- | --- |
| 6 characters (simple) | Few seconds |
| 10 characters (medium) | Hours to days |
| 12+ characters (complex) | Years to centuries |

The stronger the password, the more time it takes to crack—even with advanced tools.

### **📌 Conclusion**

Creating strong, unique passwords is the **first line of defense** against unauthorized access. This task improved my understanding of password composition, evaluation, and modern attack strategies.