|  |  |  |  |
| --- | --- | --- | --- |
| **Password** | **Strength (Rating)** | **Time to Crack** | **Tool Feedback** |
| apple123 | Weak | <1 second | Too common, predictable |
| Apple@2025 | Medium | Minutes | Needs more symbols or length |
| A$1bC!9xZ | Strong | Centuries | |  | | --- | |  |  |  | | --- | | Excellent complexity | |
| CorrectHorseBatteryStaple | Strong | Decades | Long, but lacks symbols |
| T!g3r#M@sk2025! | Very Strong | Centuries+ | Excellent entropy |
|  |  |  |  |
|  |  |  |  |

**Note Scores and Feedback from the Tool**

**Identify Best Practices for Creating Strong Passwords**

From testing and tool feedback:

* Use **12+ characters**.
* Mix **uppercase**, **lowercase**, **numbers**, and **symbols**.
* Avoid **dictionary words** or **common phrases**.
* Don't reuse passwords across accounts.
* Use **password managers** to store and generate secure passwords.

### ****Tips Learned from Evaluation****

* **Longer is better**: Length increases time to crack exponentially.
* **Passphrases** can be effective if they're random and long.
* **Symbols and numbers** significantly improve strength.
* Avoid:
  + Names, birthdays, 123456, password
  + Keyboard patterns like qwerty, asdfgh

### ****Research Common Password Attacks****

| **Attack Type** | **Description** |
| --- | --- |
| **Brute Force** | Tries all possible combinations; slow but effective over time |
| **Dictionary Attack** | Uses lists of common passwords or words |
| **Credential Stuffing** | Uses leaked passwords from other breaches |
| **Phishing** | Tricks user into giving away the password |
| **Keylogging** | Malware captures keystrokes |
| **Rainbow Table** | Uses precomputed hash tables to crack passwords |
|  |  |

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

* Complex passwords are **far harder to crack** via brute force or dictionary attacks.
* Simple passwords (e.g., hello123) are often guessed **within seconds**.
* Complexity **slows down attackers** dramatically.
* **Length + randomness** is the best defense.
* Password managers can **generate** and **store** secure credentials you don’t have to memorize.