**Password Strength Evaluation Report**

**Purpose:**

To evaluate password strength using various complexity levels and analyze how password structure affects security.

**Test Passwords on Strength Checker**

Used reputable **Password Strength Checkers** like:

* Password Monster
* Kaspersky Password Checker

**Tested Passwords & Results**

| **#** | **Password** | **Strength** | **Estimated Crack Time** | **Feedback Summary** |
| --- | --- | --- | --- | --- |
| 1 | apple123 | Weak | < 1 second | Common pattern, lowercase + numbers only |
| 2 | ApPlE2025 | Fair | ~1 minute | Better with mixed case but still predictable |
| 3 | Appl3! | Fair | ~5 minutes | Short, basic symbol use, leetspeak guessed |
| 4 | L!ght#House88 | Strong | ~2 years | Good length, symbols, and mix of characters |
| 5 | X#5rTz8!Pl9@ | Very Strong | ~millions of years | High entropy, random, long |
| 6 | summerholiday | Weak | < 1 second | Common word, no numbers or symbols |
| 7 | Tr0ub4dor&3 | Good | ~3 days | Modified dictionary word, leetspeak pattern |
| 8 | P@55w0rd! | Very Weak | < 1 second | Common substitution, easily guessed |
| 9 | M&xT93\*vLk2P@ | Very Strong | ~trillions of years | Excellent complexity and length |
| 10 | Password123 | Very Weak | < 1 second | One of the most common passwords |

**Explanation of Password Strength Ratings**

**Weak / Very Weak**

* **Example:** apple123, Password123
* **Issues:** Short, predictable, common words or patterns, low character variety.
* **Vulnerable to:** Dictionary attacks, brute force.

**Fair / Good**

* **Example:** ApPlE2025, Tr0ub4dor&3
* **Improvements:** Used of upper/lower case and some symbols.
* **Still vulnerable to:** Pattern recognition, educated guesses.

**Strong / Very Strong**

* **Example:** L!ght#House88, X#5rTz8!Pl9@, M&xT93\*vLk2P@
* **Strengths:** Long length, high entropy, randomness, use of all character types.
* **Resistant to:** Brute force, dictionary attacks, guessing.

**Best Practices for Strong Passwords**

1. **Use at least 12–16 characters**
2. **Include uppercase, lowercase, numbers, and special symbols**
3. **Avoid dictionary words or predictable patterns**
4. **Do not use common substitutions (@ for a, 0 for o, etc.)**
5. **Avoid reusing passwords across platforms**
6. **Use a password manager to generate and store passwords**

**How Complexity Improves Security**

* **More characters** exponentially increase crack time.
* **Unpredictable symbols** and **random sequences** block dictionary and pattern-based attacks.
* **High entropy** means the password doesn’t follow human-like logic—harder for attackers to guess.

**Conclusion**

Password strength is not just about including symbols—**length**, **randomness**, and **unpredictability** are crucial. Avoid using memorable but guessable phrases. Instead, use **complex, long, and unique passwords** for maximum security.