Password Strength Evaluation Report

1. Introduction: The Critical Role of Password Strength

The goal of this task was to gain a practical understanding of password construction and empirically test what makes a password truly strong. In the current digital landscape, a robust password is the first and most vital defense against account takeovers and data breaches. By analyzing test results, this report aims to confirm best security practices and explain how complexity directly impacts overall safety.

2. Password Evaluation Methodology

- **Tool Used:** The online free password strength checker used for this evaluation was based on the provided hint **(similar to passwordmeter.com).**
- **Method:** Three passwords with intentionally varying complexity (length, character types, and randomization) were created and tested. The scores, complexity rating, additions, and deductions provided by the tool were recorded for analysis.

3. Password Test Results and Analysis

The tests revealed a clear, dramatic improvement in password strength directly tied to increased complexity:

My first test used the simple 8-character password, **doggy123**. This password, relying only on lowercase letters and sequential numbers, was rated as **Weak** with a score of **37%**. The tool assigned significant penalties for its lack of symbols and mixed case, but more importantly, for predictable sequences like consecutive letters (ggy) and numbers (123). This result confirms that short, predictable strings are easily cracked.

The second attempt, **Password25**, showed improvement by increasing the length to 10 characters and introducing one uppercase letter. This resulted in a **Strong** rating of **66%**. While better, it still fell short because the core of the word is a widely-used dictionary term, which led to minor deductions. This demonstrated that simply meeting minimum requirements isn't enough; attackers anticipate simple substitutions and capitalization.

The final and most successful password was the 11-character **P@sswOrd!25**. By strategically incorporating characters from **all four major categories**—uppercase, lowercase, numbers, and multiple symbols (@ and !)—the password achieved the maximum score of **100% / Very Strong**. The sheer variety provided a massive security bonus, effectively neutralizing any minor deductions. The takeaway is that **length is the foundation, but comprehensive character variety is what creates true resilience.**

4. Best Practices and Tips Learned

The evaluation process highlighted clear principles for maximum security:

First, **length is non-negotiable**. The strongest protection comes from long passwords, preferably 12 characters or more, structured as easily memorable but unpredictable passphrases. Second, **symbols are highly effective**; the addition of special characters provides the biggest measured jump in security. Third, always **avoid using any common dictionary words, names, or simple keyboard sequences** (like qwerty or 12345), as these are the first things cracking software will test. Finally, the most critical tip is to **use a unique, strong password for every single account** to prevent a widespread system compromise if one service is breached.

5. Common Password Attacks and Security Summary

A complex password defends against a variety of sophisticated attacks, not just simple guessing. While the two classic techniques are **Brute Force** (trying every possible combination) and the **Dictionary Attack** (trying common words), modern threats are often more human-centered:

- **Credential Stuffing** exploits the weakness of **password reuse**. Attackers take large lists of usernames and passwords stolen from one compromised website and automatically try them on various other sites, assuming the victim used the same login everywhere.
- **Phishing and Social Engineering** attacks circumvent the password entirely by tricking the user (often via fake emails or login pages) into **voluntarily handing over** their credentials.
- **Keylogger Attacks** are malware designed to record every single keystroke the user makes, capturing the password as it is typed before it is even transmitted.

In summary, password complexity and uniqueness are the only effective counters to this diverse threat landscape. Complexity makes automated cracking attempts too slow to be feasible. Uniqueness, combined with the implementation of **Multi-Factor Authentication (MFA)**, breaks the chain of vulnerability exploited by credential stuffing and phishing, ensuring that a single compromised password does not lead to an entire identity theft.