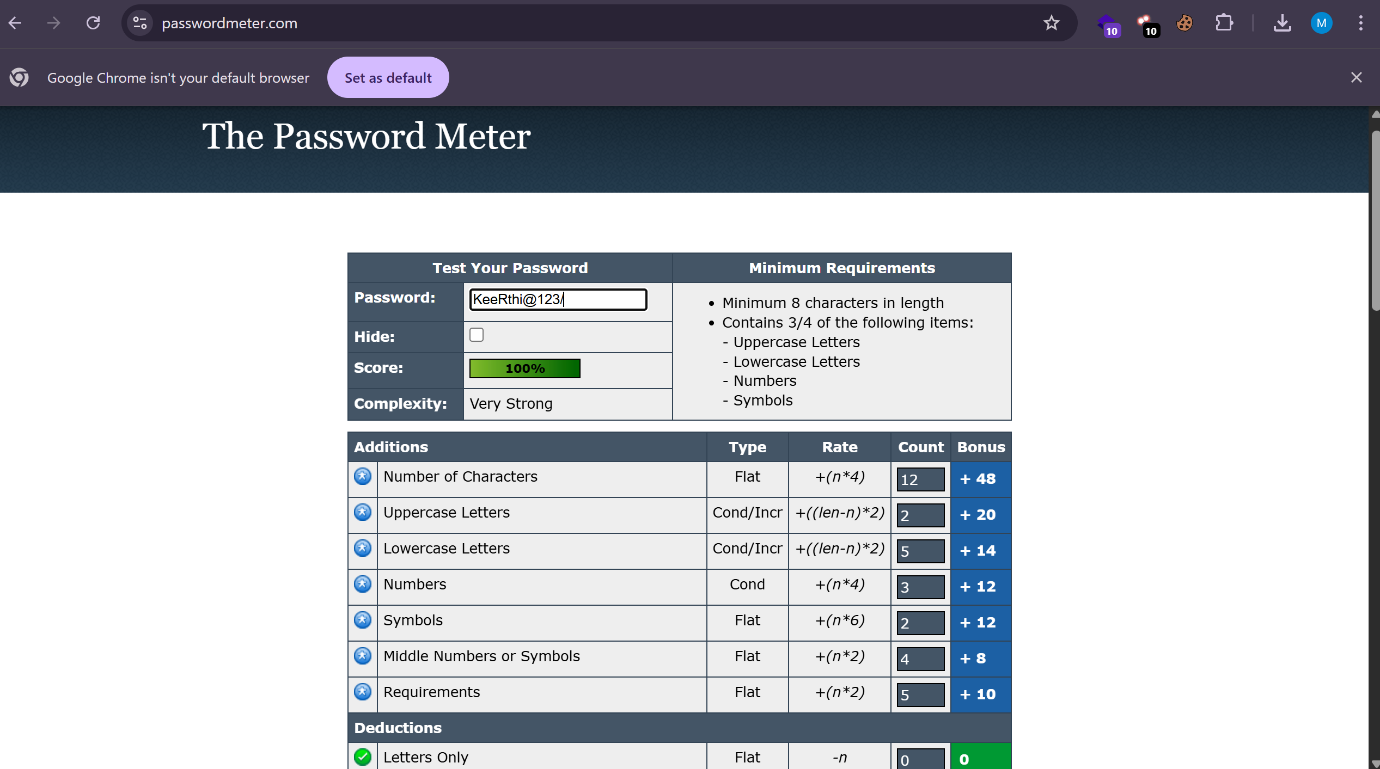
**Task 6 : Create a Strong Password and Evaluate Its Strength**.



A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

* **Best Practices for Creating Strong Passwords**
* Use at least 12–16 characters.
* Include uppercase, lowercase, numbers, and symbols.
* Avoid dictionary words or common substitutions (like 'Pa$$w0rd').
* Use random, non-predictable sequences.
* Do not reuse passwords across sites.
* **Tips Learned from Evaluation**
* Short passwords—even with numbers—are weak.
* Adding **symbols and mixing character types** significantly increases strength.
* Randomness and length are more important than clever substitutions.
* Passwords based on **phrases or passphrases** (e.g., “GiraffesEat^Clouds4Lunch!”) can be strong and easier to remember.
* Use a **password manager** to generate and store complex passwords.
* **Common Password Attacks**
* **Brute Force Attack**: Attempts every possible combination. Mitigated by longer, more complex passwords.
* **Dictionary Attack**: Uses common words and known passwords. Avoid dictionary words to defend.
* **Credential Stuffing**: Uses leaked credentials from other sites. Prevented by using **unique passwords** per site.
* **Phishing**: Social engineering to steal credentials. Doesn’t depend on complexity—user vigilance and 2FA are key.
* **How Password Complexity Affects Security**

Password complexity increases the number of possible combinations, which directly resists brute-force and dictionary attacks. Each additional character **exponentially increases** the effort required to crack it. For example:

* A 6-character lowercase password has ~308 million combinations.
* A 16-character mixed-type password can have **over 10⁹²** combinations.

Greater complexity reduces guessability, making automated attacks impractical—especially when paired with **multi-factor authentication** and unique usage.