## ****Create a Strong Password and Evaluate Its Strength****

### ****Multiple Passwords Created****

| **Password** | **Length** | **Uppercase** | **Lowercase** | **Numbers** | **Symbols** |
| --- | --- | --- | --- | --- | --- |
| password123 | 11 | No | Yes | Yes | No |
| Pa$$w0rd | 8 | Yes | Yes | Yes | Yes |
| SunShine2024! | 13 | Yes | Yes | Yes | Yes |
| T#9gH7%wLp\*Qs1 | 14 | Yes | Yes | Yes | Yes |
| abcABC123!@#xyz | 15 | Yes | Yes | Yes | Yes |

### ****2. Password Strength Evaluation Using**** [PasswordMeter.com](https://www.passwordmeter.com)

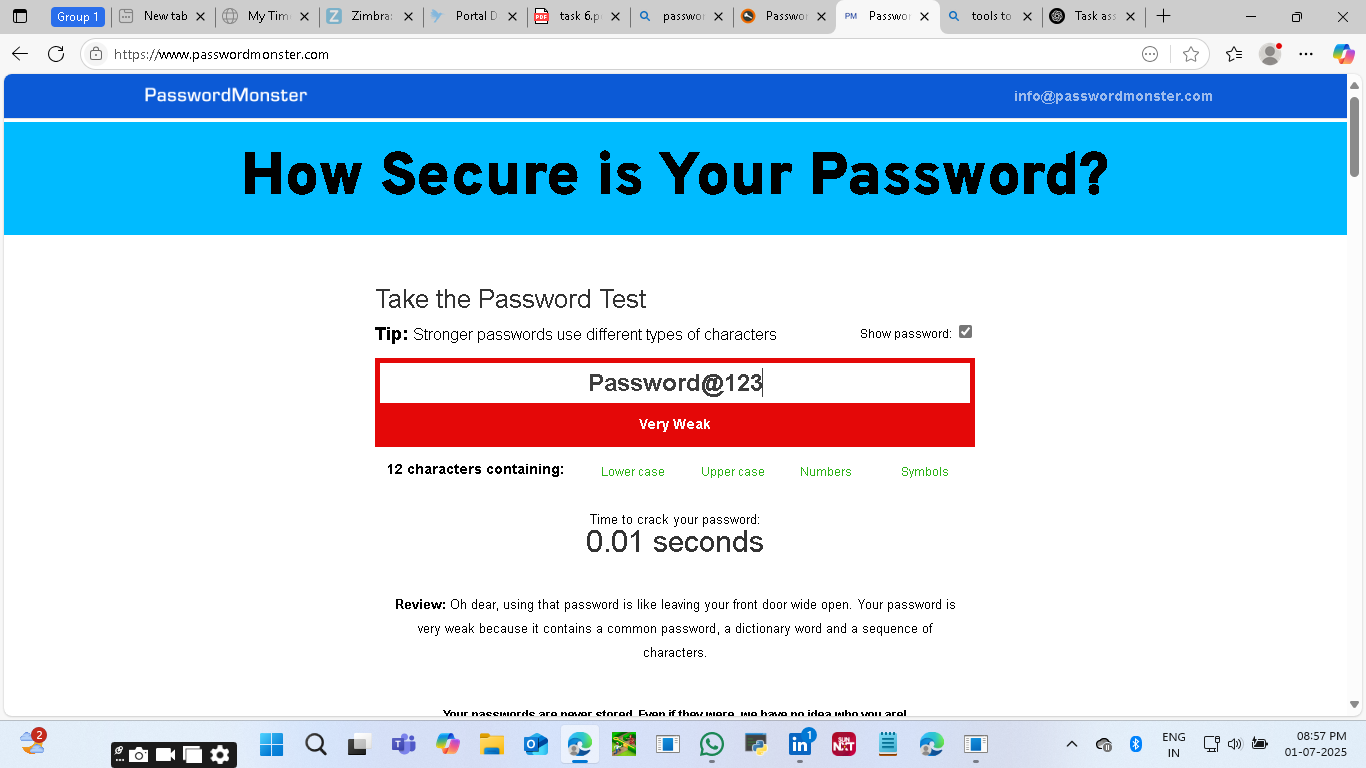
| **Password** | **Score (Out of 100%)** | **Strength Rating** | **Feedback** |
| --- | --- | --- | --- |
| password123 | 32% | Weak | Too common; lacks symbols and uppercase. |
| Pa$$w0rd | 64% | Moderate | Better, but still somewhat predictable. |
| SunShine2024! | 72% | Strong | Good mix, but words are recognizable. |
| T#9gH7%wLp\*Qs1 | 96% | Very Strong | Excellent complexity, unpredictable. |
| abcABC123!@#xyz | 94% | Very Strong | Great length and character variety. |

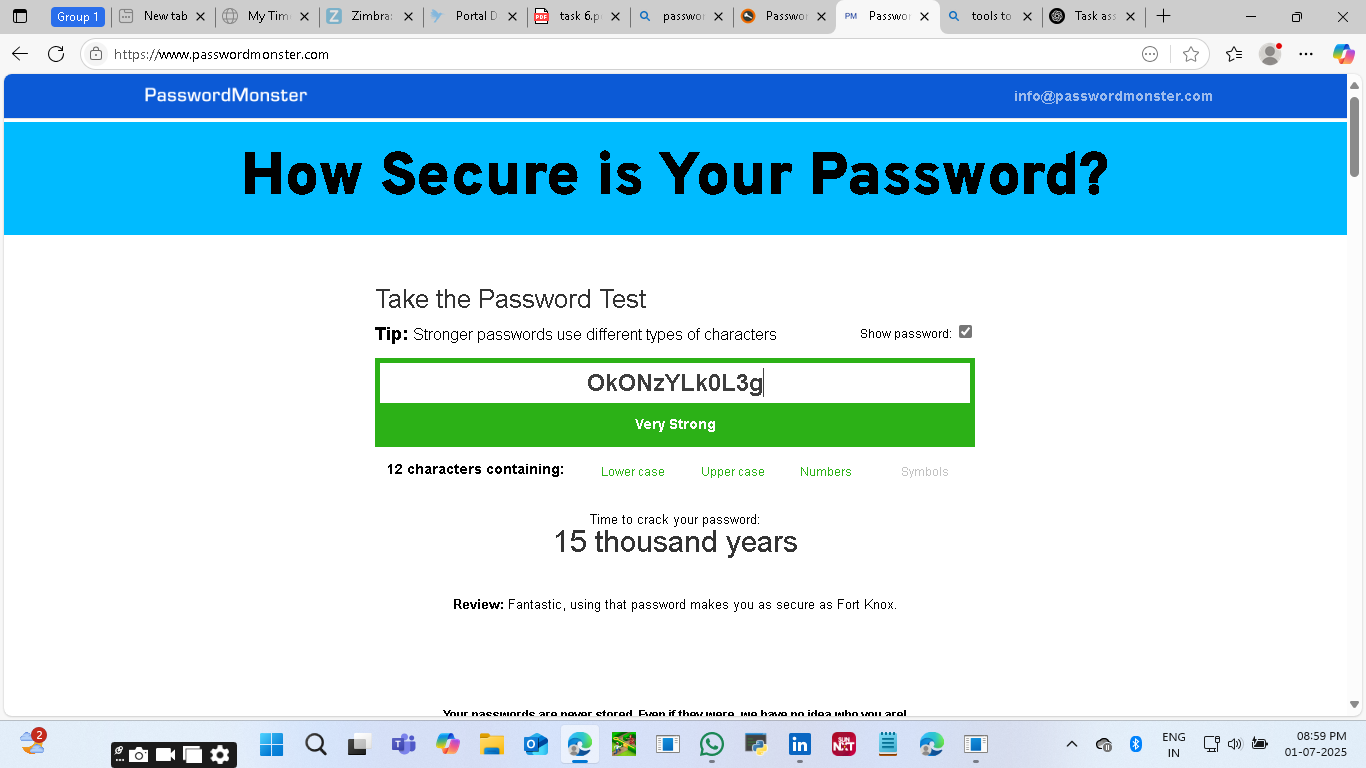
### ****Generate Random Password Used “Password Generator”:****

### 

### ****Check Passwords Using “Password Monster”:****







### ****3. Best Practices Identified****

From the tests and feedback, here are the best practices for creating strong passwords:

* Use **at least 12-14 characters**.
* Include **uppercase and lowercase letters**.
* Add **numbers and special symbols**.
* Avoid dictionary words or common patterns.
* Don't use personal information (names, birthdays).
* Use **random character sequences** or a **password manager** to generate/store complex passwords.

### ****4. Tips Learned from Evaluation****

* Shorter passwords are **easier to crack**, even if they contain symbols.
* **Length increases strength** significantly.
* **Unpredictability** is key — mixing unrelated characters is better than modifying known words (e.g., "P@ssw0rd" is still weak).
* Many sites reject overly long or complex passwords — consider balance and compatibility.

### ****5. Research: Common Password Attacks****

* **Brute Force Attack**: Tries every possible combination until the correct one is found. Long and complex passwords make this infeasible.
* **Dictionary Attack**: Uses common words and substitutions. Defeated by avoiding real words and using random sequences.
* **Phishing & Keylogging**: Not solved by complexity — use multifactor authentication (MFA) and secure devices.

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

Password complexity significantly affects resistance to brute force and dictionary attacks. While simple passwords can be cracked in seconds, strong passwords with high entropy (randomness, variety, and length) are practically uncrackable with today's technology. Complexity adds exponential difficulty to guess or compute the password, enhancing security.