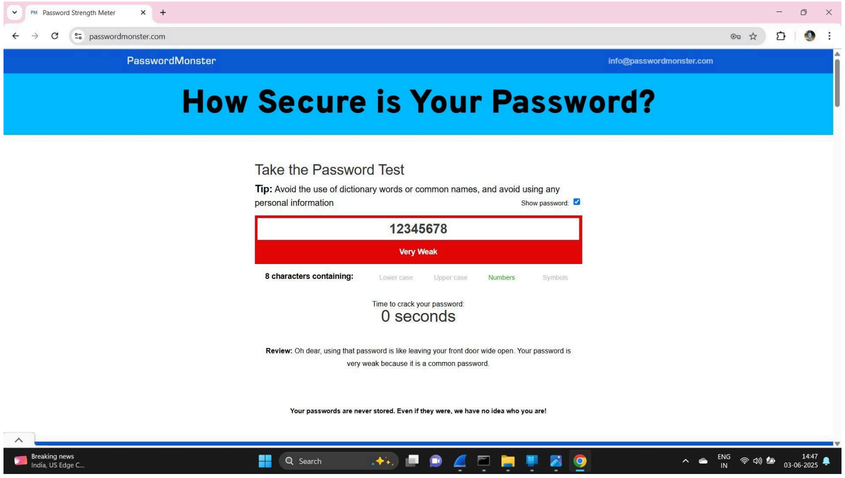
Creating a Strong Password and Evaluating Its Strength

Objective:To understand what makes a password strong and test it using password strength tools.

1. Password Strength Evaluation

To evaluate password strength, I tested three different passwords using an online tool.

- The first password, '12345678', consisted only of numbers and was very weak. It could be cracked in 0 seconds and is considered a common, easily guessable password.



How Secure is Your Password?

Take the Password Test

Tip: Avoid the use of dictionary words or common names, and avoid using any personal information

Show password: ☑

12345678

Very Weak

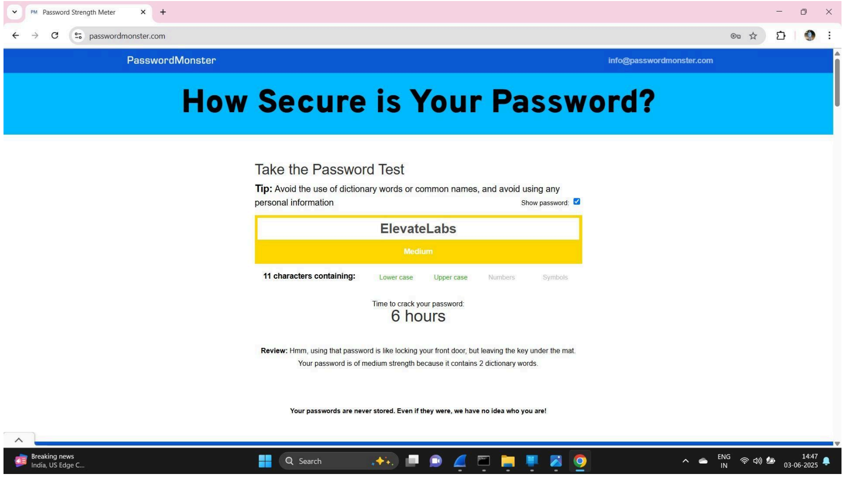
8 characters containing: Lower case Upper case Numbers Symbols

Time to crack your password:
0 seconds

Review: Oh dear, using that password is like leaving your front door wide open. Your password is very weak because it is a common password.

Your passwords are never stored. Even if they were, we have no idea who you are!

- The second password, 'ElevateLabs', used a combination of uppercase and lowercase letters and was evaluated as medium strength. Despite being longer, it contained dictionary words and could be cracked in approximately 6 hours.



How Secure is Your Password?

Take the Password Test

Tip: Avoid the use of dictionary words or common names, and avoid using any personal information

Show password: ☑

ElevateLabs

Medium

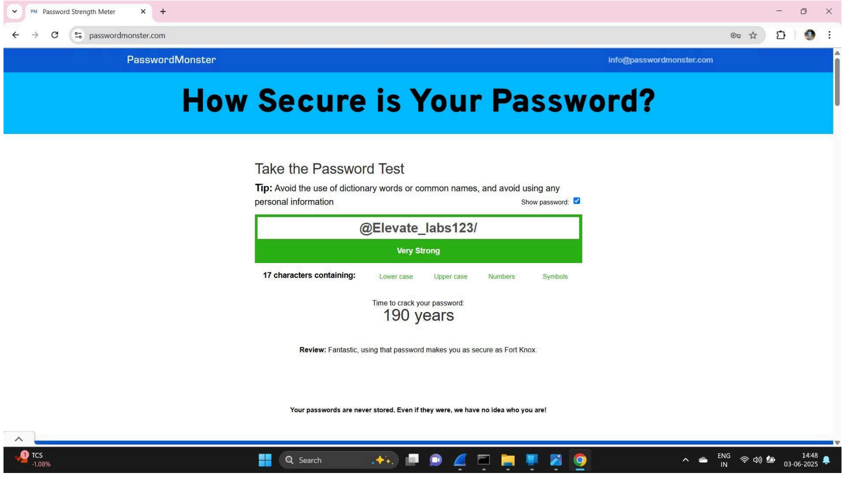
11 characters containing: Lower case Upper case Numbers Symbols

Time to crack your password:
6 hours

Review: Hmm, using that password is like locking your front door, but leaving the key under the mat. Your password is of medium strength because it contains 2 dictionary words.

Your passwords are never stored. Even if they were, we have no idea who you are!

- The final password, '@Elevate_labs123/', included uppercase and lowercase letters, symbols, and numbers. With a length of 17 characters, this password was rated very strong with an estimated crack time of 190 years. Its complexity and length made it highly secure.



How Secure is Your Password?

Take the Password Test

Tip: Avoid the use of dictionary words or common names, and avoid using any personal information

Show password: ☑

@Elevate_labs123/

Very Strong

17 characters containing: Lower case Upper case Numbers Symbols

Time to crack your password:
190 years

Review: Fantastic, using that password makes you as secure as Fort Knox.

Your passwords are never stored. Even if they were, we have no idea who you are!

2. Observations and Learnings

Password complexity is influenced by several factors. Longer passwords are exponentially harder to crack. Including a variety of characters such as uppercase letters, lowercase letters, numbers, and symbols significantly improves strength. Unpredictability is also crucial—dictionary words and common patterns like '123456' should be avoided.

Best practices for creating strong passwords include using more than 12 characters, mixing different types of characters, avoiding personal information such as names or birthdates, not reusing passwords across multiple sites, and utilizing passphrases or random word combinations with symbols and numbers.

3. Common Password Attacks

There are several common types of password attacks.

- Brute force attacks attempt every possible character combination until the correct one is found.
- Dictionary attacks use predefined lists of common words and phrases to guess passwords.
- Credential stuffing involves using usernames and passwords leaked from other data breaches.

4. Importance of Password Length

Password length plays a vital role in security. Each additional character increases the number of possible combinations exponentially. For instance, a 17-character password with mixed elements offers far greater security than an 8-character password.

5. Security Tools Used

The password strength was evaluated using the online tool PasswordMonster.com.

6. Tips Learned

Through this task, I learned that a password like '@Elevate_labs123/' is almost impossible to crack due to its length and complexity. Conversely, even a professional-sounding password like 'ElevateLabs' is vulnerable if it includes dictionary words. Short numeric passwords are particularly risky and should be strictly avoided.

7. Final Verdict

Password strength checkers are essential for assessing how secure a password is. This task highlighted the importance of creating long, complex, and unique passwords. Understanding these principles is fundamental for both cybersecurity professionals and personal data protection.