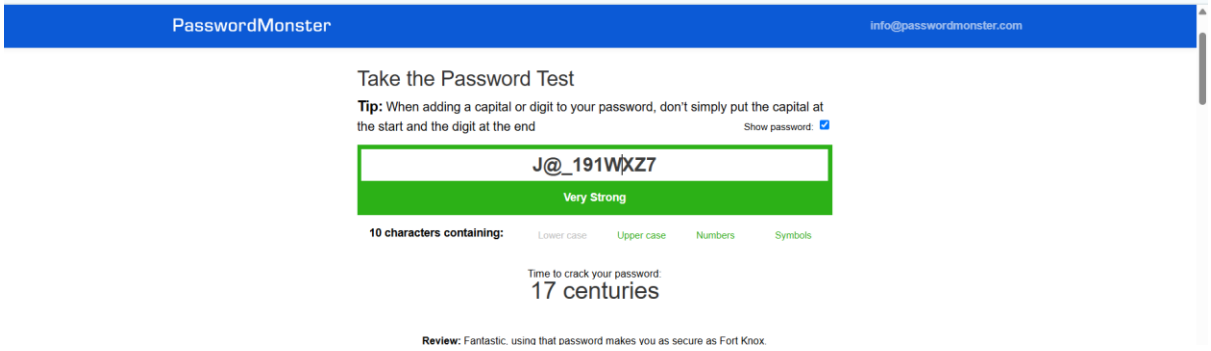
TASK-6 Password Strength Evaluation

Step 1: Creating Multiple Passwords with varying complexity. Here are 5 examples passwords with increasing complexity.

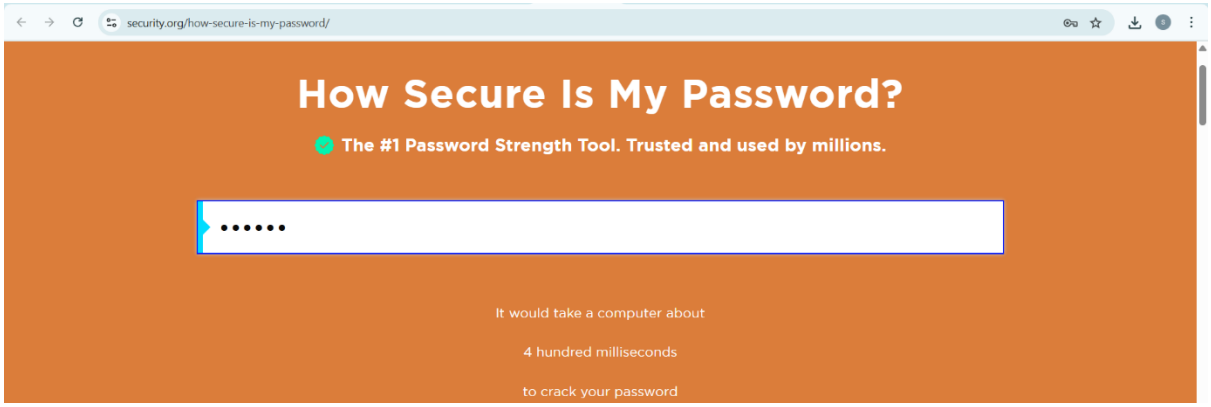
Password Evaluation:

Step 2: Here I used the online website Password Monster to check the complexity of the password.

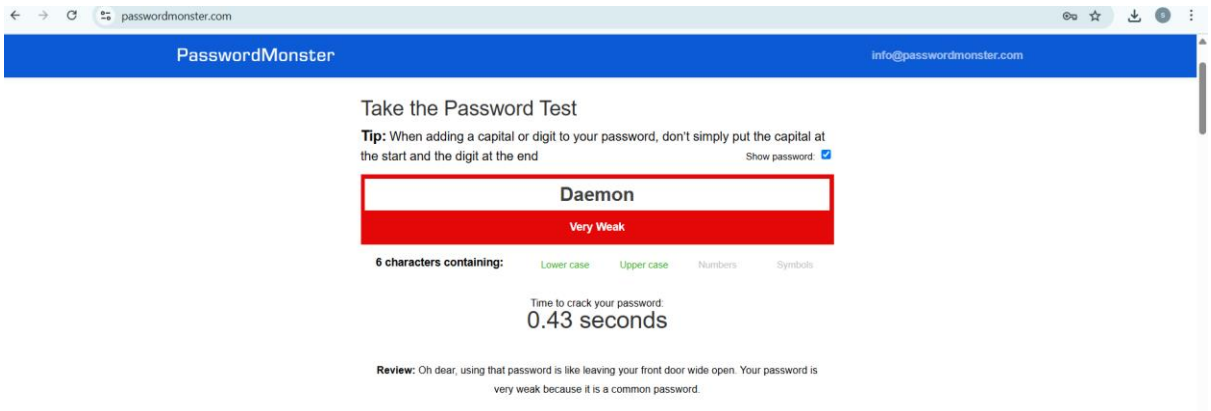
I created a password with 10 characters using Uppercase, Lowercase, Special Characters and Numbers.



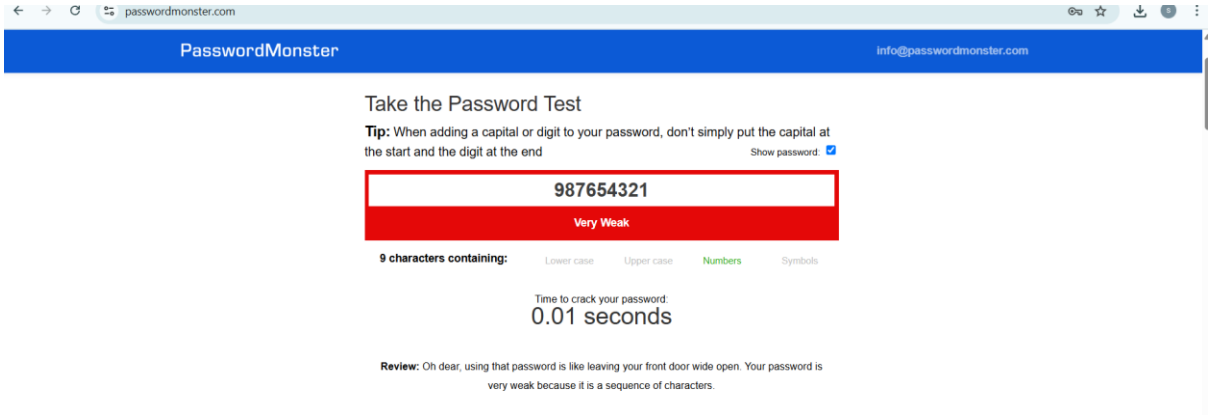
Step 3: I created Password (i.e. Daemon) with just 6 characters with upper case, lower case. Here I checked the password in Online website named How Secure Is My Password.com.

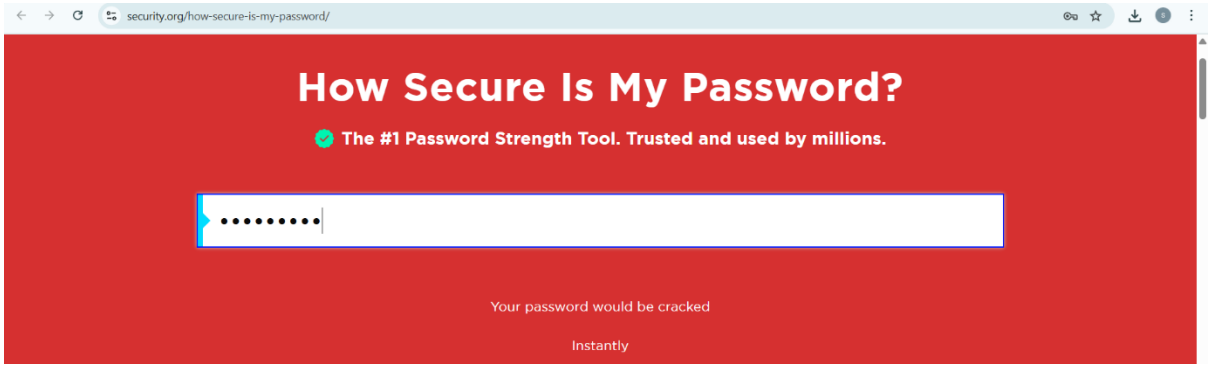


Also checked with another website named Password Monster to check the complexity of that password.

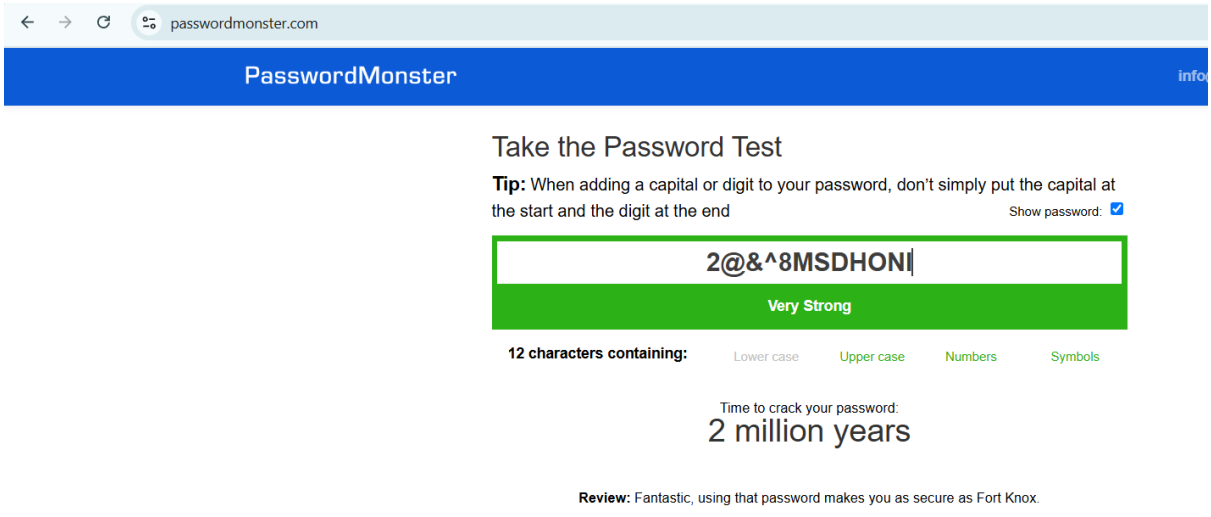


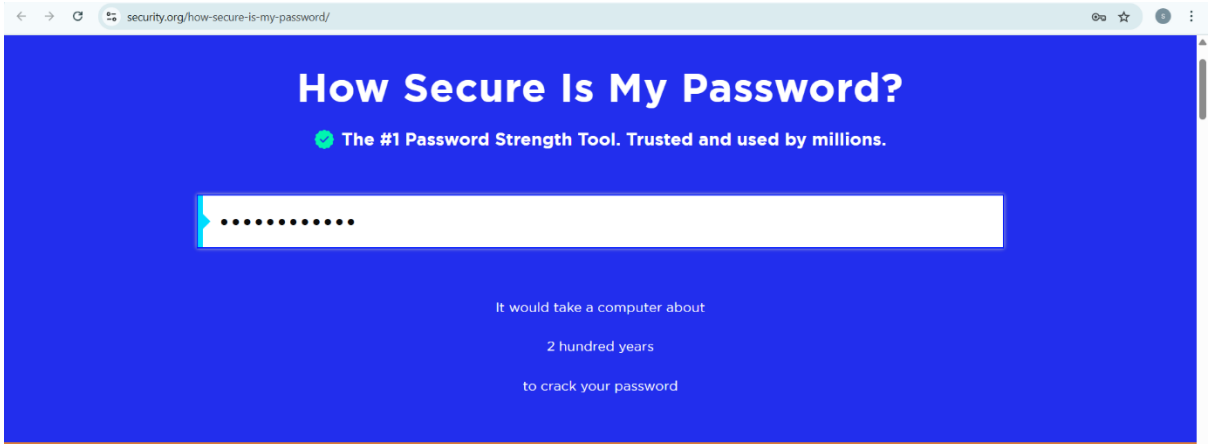
Step 4: Here I created a password with only numbers to check the complexity of the password in different websites.





Step 5: Creating a strong password by starting with a Number and ending with Uppercase and in between them placed special characters.





Based on tools feedback, using a mix of characters and making passwords at least 12-16 characters long. Avoiding dictionary words or common phrases.

Example tips:

1. Avoid names and dates.
2. Longer is stronger.
3. Use random words.

Common Password Attacks

Password attacks are a significant threat to cybersecurity, allowing unauthorized access to systems and sensitive data. Here are some of the most common types:

- **Brute-Force Attacks:** This involves systematically trying every possible combination of characters until the correct password is found. Automated tools can rapidly test millions of combinations per second.
- **Dictionary Attacks:** A more refined brute-force method, this attack uses pre-compiled lists of common words, phrases, and previously leaked passwords. Attackers often combine dictionary words with numbers and special characters (e.g., substituting 'o' with '0').
- **Credential Stuffing:** This attack leverages lists of stolen username and password combinations from previous data breaches. Attackers "stuff" these credentials into login pages of other sites, banking on users reusing the same passwords across multiple platforms.
- **Phishing:** Attackers trick users into voluntarily revealing their credentials. This often involves sending fraudulent emails or creating fake login pages that mimic legitimate websites, coaxing users to enter their sensitive information.
- **Keylogging:** Malware is installed on a user's device that records every keystroke, including usernames and passwords. This information is then sent to the attacker.
- **Man-in-the-Middle (MitM) Attacks:** An attacker intercepts communication between a user and a legitimate website or application. This allows them to capture login credentials transmitted over unsecured networks (e.g., public Wi-Fi).
- **Password Spraying:** Instead of targeting a single account with many password guesses (like brute-force), this attack tries a small number of common passwords against a large number of user accounts to avoid triggering account lockouts.

- **Rainbow Table Attacks:** This technique targets hashed passwords (passwords converted into a fixed-length, unreadable string). Attackers use pre-computed tables of hash values to quickly find the original plaintext password that corresponds to a stolen hash.
- **Social Engineering:** This involves manipulating human behaviour to trick individuals into revealing sensitive information, including passwords. Phishing is a prime example, but it can also include phone calls (vishing) or text messages (smishing).

How Password Complexity Affects Security:

Password complexity, which involves length and variety of characters, significantly impacts security by making it harder for attackers to guess or crack passwords. Longer, more complex passwords take longer to crack, making them less likely to be compromised by brute-force or dictionary attacks.

Here's a more detailed explanation:

Length:

Longer passwords have a larger number of possible combinations, making them more difficult to crack with brute-force methods. A 12-character password takes 62 trillion times longer to crack than a 6-character password, according to JumpCloud.

Character Variety:

Using a mix of uppercase and lowercase letters, numbers, and symbols further increases the complexity and makes it harder for attackers to guess or crack the password.

Unpredictability:

Avoiding common words, phrases, or easily guessable personal details improves password complexity and reduces the chance of being guessed or cracked by dictionary attacks.

Benefits of Complexity:

By increasing complexity, password policies help enforce the use of unique and secure passwords, making them more difficult to crack. This, in turn, reduces the risk of unauthorized access to sensitive information and accounts.

Drawbacks of Complexity:

While complexity is important, excessive complexity can lead to users creating weak passwords or reusing them across multiple accounts. It's also important to remember that all passwords can be cracked with enough time and computing power, so the goal should be to make them difficult to crack, not uncrackable.