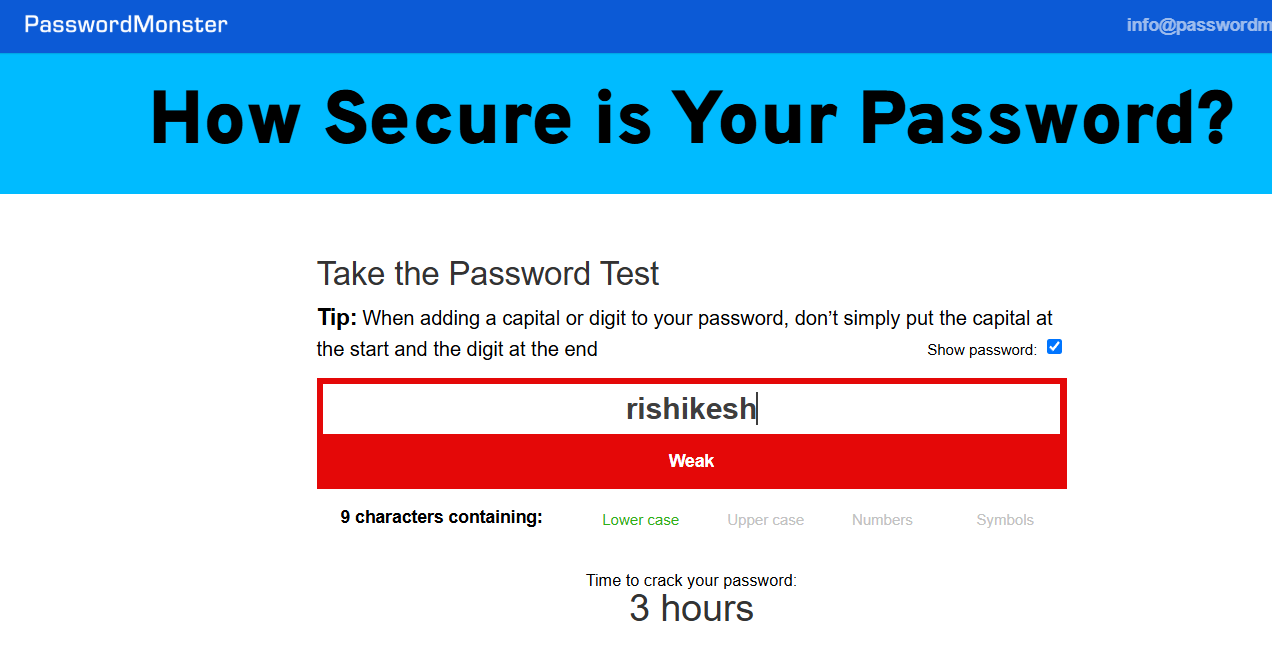
PASSWORD STRENGTH ANALYSIS

Submitted by

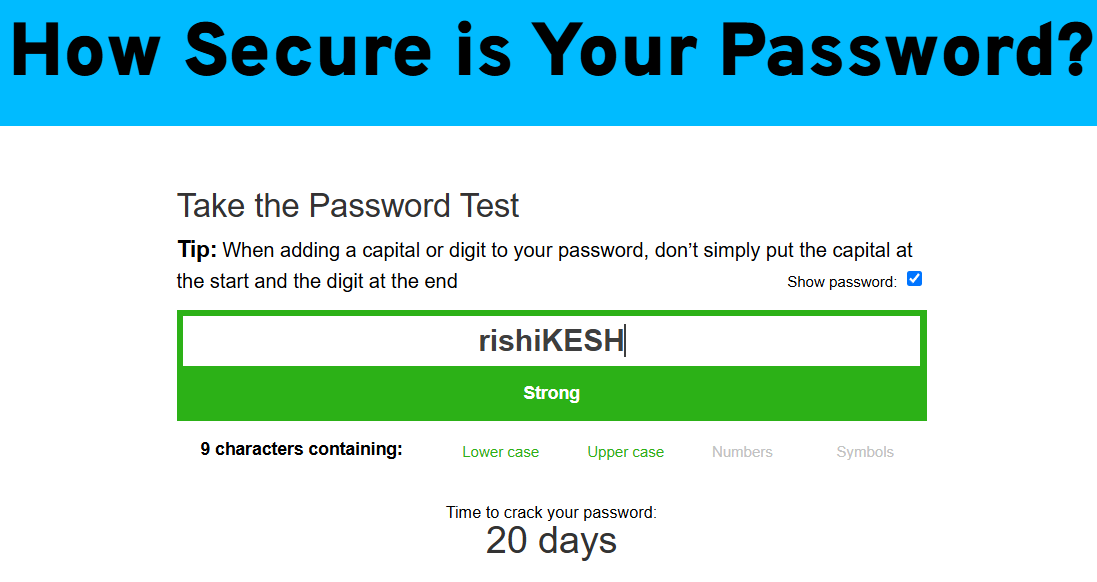
Rishikesh M

**Using the website** [**https://www.passwordmonster.com/**](https://www.passwordmonster.com/) **, we can evalutate the strength of passwords easily.**

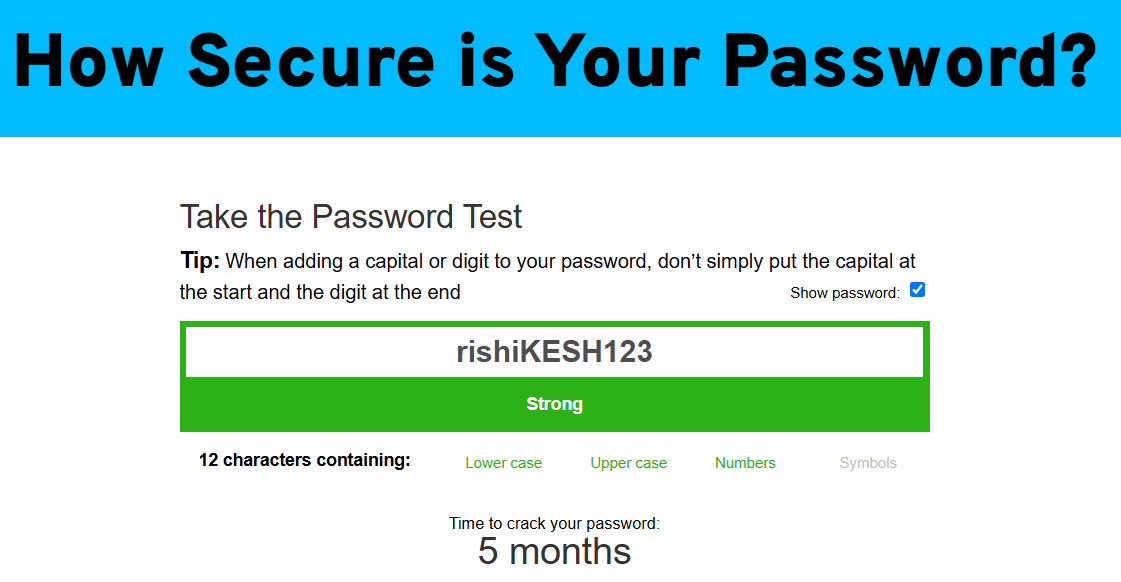
Using my name as a password with all characters as lowercase, gives a very weak password.



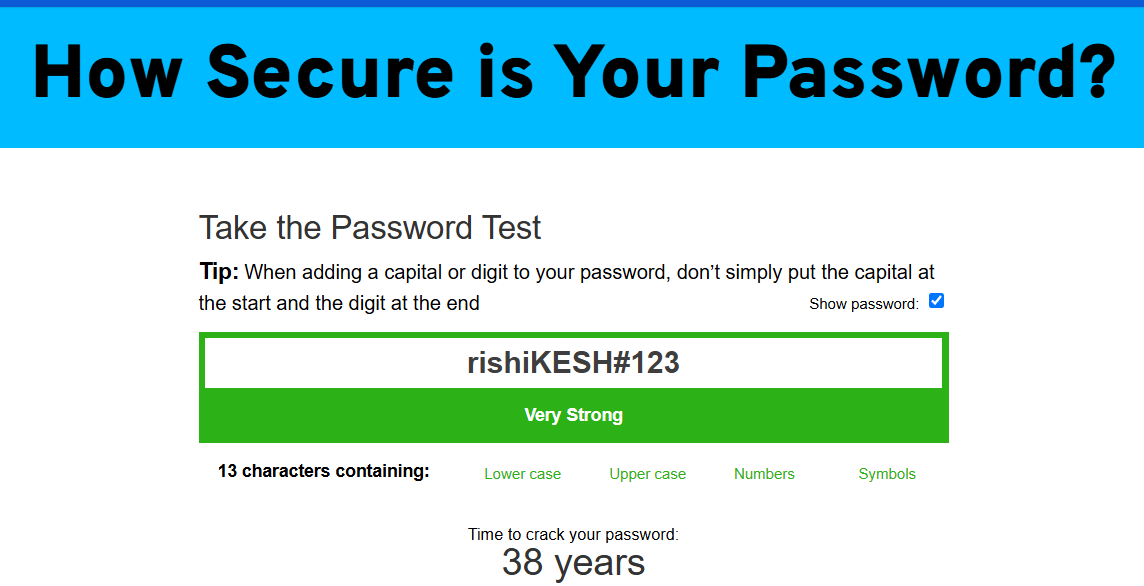
Using uppercase characters mixed with lowercase increases the strength of the password.



Using numbers along with the above example makes it change from 20 days to 5 months to crack the password.



To increase the complexity further, special characters can be added which makes the password near impossible to crack.



BEST PRACTICES IN PASSWORD CREATION

1. Make them long.

2. Make them random eg: Yuc8$RikA34%ZoPPao98t.

3. Not a word that can be found in a dictionary or the name of a person, character, product, or organization.

4. Should be Significantly different from your previous passwords.

5. Use a unique password for each website.

6. Use password managers with random passwords generated by them.

7. Leetspeak is common in passwords. Leetspeak is when standard letters are often replaced by numerals or special characters that resemble the letters

COMMON PASSWORD ATTACKS

**Brute Force and Dictionary Attacks**

This is a trial and error method in which the attacker uses a list of common passwords either available on the internet or custom tailored for the targeted user against the website. This is a tedious process and requires an extensive amount of computing power. These lists come from leaked databases, password-cracking tools etc.  Tools like Hashcat and John the Ripper combine the powers of brute force and dictionary techniques, allowing attackers to target multiple accounts at once. Reverse brute force attacks use known or stolen passwords to uncover corresponding usernames.



SUMMARY

Passwords are the values that websites use as authentication tokens to identify and secure the sessions of the different users present. These can be easily acquired by attackers with malicious intent using attacks like bruteforce, dictionary, keyloggers etc. This creates the need to create better and complex passwords that cannot be targeted by attackers easily. The best practices to create passwords in this presentation serves as a basic guideline for any user in creating passwords in the future. The main benefit of password complexity rules is that they enforce the use of unique passwords that are harder to crack.

REFERENCES

<https://www.passwordmonster.com/>

<https://www.cisa.gov/secure-our-world/use-strong-passwords>

<https://support.microsoft.com/en-us/windows/create-and-use-strong-passwords-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb>

<https://bitwarden.com/password-strength/>