

REPORT

→ Password, their strengths and feedback details of the tool.

<u>Password</u>	<u>Strength</u>	<u>Length</u>	<u>Time to Crack</u>	<u>Out of</u> <u>(N,S,UC,LC)</u>
jinendrasharma	Strong	14	2 months	2
asdf@#Jinendra	V.Strong	14	42 yrs	3
Jine\$%ndra12	V.Strong	12	759 yrs	All
Rishi@#\$ihSiR	V.Strong	13	23 yrs	3
Rishi@#23ihSiR	V.Strong	14	14 centuries	All
Jinendra@12345246	V.Strong	17	20 centuries	All
Jinendra123456789	Medium	17	2 days	3
Jine123456789ndra	Strong	17	7 months	3
123456789Jinendra	Medium	17	2 days	3
12345Jinendra6789	Strong	17	1 month	3
12345Jine6789ndra	V.Strong	17	8 yrs	3
12Ji345ne67ndra89	V.Strong	17	90 Billion yrs	3

Important Note- N, S, UC, LC stands for Numbers, Symbols,
Uppercase, Lowercase respectively.

2.Best practices to create strong passwords

- Password should atleast 12 characters long.
- Should include numbers, symbols, uppercase and lowercase letters.
- Should be random and unpredictiable.
- Avoid Personal information in your password.
- Check strength of password online then only use it.
- Use MFA(Multi Factor authentication) to add a extra layer of security to your account from being hacked.

3. How Complexity Strengthens Security

1. Resistance to Brute-Force Attacks

- Brute-force attacks try every possible combination.
- A simple 6-character password with only lowercase letters has **308 million possible combinations.**
- A 12-character password mixing uppercase, lowercase, numbers, and symbols has **over 10^{21} combinations,** making brute-force practically impossible.

2. Defense Against Dictionary Attacks

- Attackers often use lists of common words or leaked passwords.
- Adding complexity (symbols, numbers, mixed case) makes passwords less predictable and less likely to appear in these lists.

3. Protection from Credential Stuffing

- Reused or simple passwords are easily exploited in credential-stuffing attacks.
- Complex, unique passwords reduce the chance of being compromised across multiple accounts.

4. Policy Enforcement

- Systems like Windows enforce complexity rules (e.g., disallowing usernames or full names in passwords) to prevent weak, guessable credentials.

Brute force and Dictionary attacks—

1.Brute force attack- It is basically a type of attack in which attacker tries every possible combination of password to crack the password. It purely depends on computing power and inefficient as well.

2.Dictionary attack- In this type of attack, we give a list of word to the attacking software and it tries each password can be formed from the words are present in the dictionary and it is a better option than brute force attack. But it is also inefficient for lengthy and random passwords.

Appendix

The image displays three separate screenshots of a web browser window, each showing the results of a password strength test on the "How Secure is Your Password?" page of the PasswordMonster website (passwordmonster.com). The browser interface includes a toolbar at the top, a address bar, and a status bar at the bottom showing network and battery information.

Screenshot 1: The first screenshot shows a password of "asdf@#Jinendra". The analysis indicates it is "Very Strong" and contains 14 characters, including symbols. The estimated time to crack the password is 42 years. A review states: "Review: Fantastic, using that password makes you as secure as Fort Knox."

Screenshot 2: The second screenshot shows a password of "Jine\$%ndra12". The analysis indicates it is "Very Strong" and contains 12 characters, including symbols. The estimated time to crack the password is 759 years. A review states: "Review: Fantastic, using that password makes you as secure as Fort Knox."

Screenshot 3: The third screenshot shows a password of "Rishi@#\$ihsIR". The analysis indicates it is "Very Strong" and contains 13 characters, including symbols. The estimated time to crack the password is 23 years. A review states: "Review: Fantastic, using that password makes you as secure as Fort Knox."

The screenshot shows a password strength test for the password "Rishi@#23ihsIR". The result is "Very Strong" with a green bar. It contains 14 characters, including lowercase, uppercase, numbers, and symbols. The estimated cracking time is 14 centuries.

Take the Password Test
Tip: Stronger passwords use different types of characters Show password

Rishi@#23ihsIR

Very Strong

14 characters containing: Lower case Upper case Numbers Symbols

Time to crack your password: 14 centuries

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

The screenshot shows a password strength test for the password "Rishi@#23ihsIR". The result is "STRONG" with a green bar. It contains 14 characters, including lowercase, uppercase, numbers, and symbols. The estimated cracking time is centuries.

Take a moment to check if your passwords are easy pickings for bad actors
Rishi@#23ihsIR

Password strength: STRONG

Time it takes to crack your password: centuries

Password composition
Make sure that your password is long enough and contains various types of characters.
 At least 12 characters
 Lowercase
 Uppercase
 Symbols (!@#\$...)
 Numbers

Has this password been previously exposed in data breaches?

The screenshot shows a password strength test for the password "Jinendra@12345246". The result is "Very Strong" with a green bar. It contains 17 characters, including lowercase, uppercase, numbers, and symbols. The estimated cracking time is 20 centuries.

Take the Password Test
Tip: Stronger passwords use different types of characters Show password

Jinendra@12345246

Very Strong

17 characters containing: Lower case Upper case Numbers Symbols

Time to crack your password: 20 centuries

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

The screenshot shows a password strength test for the password "Jinendra123456789". The result is "Medium" with a yellow bar. It contains 17 characters, including lowercase, uppercase, numbers, and symbols. The estimated cracking time is 2 days.

Take the Password Test
Tip: Stronger passwords use different types of characters Show password

Jinendra123456789

Medium

17 characters containing: Lower case Upper case Numbers Symbols

Time to crack your password: 2 days

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 3 dictionary words and a sequence of characters.

The image displays three vertically stacked screenshots of the PasswordStrength Meter website, specifically the "How Secure is My Password?" page. Each screenshot shows a different password being analyzed.

Screenshot 1: The password entered is "Jine123456789ndra". The result is "Strong" with a green bar. It contains 17 characters, including lowercase, uppercase, numbers, and symbols. The estimated crack time is 7 months. A review states: "Good, using that password is like locking your front door and keeping the key in a safety deposit box."

Screenshot 2: The password entered is "123456789Jinendra". The result is "Medium" with a yellow bar. It contains 17 characters, including lowercase, uppercase, numbers, and symbols. The estimated crack time is 2 days. A review states: "Hmmm, 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 a sequence of characters and 3 dictionary words."

Screenshot 3: The password entered is "12345Jinendra6789". The result is "Strong" with a green bar. It contains 17 characters, including lowercase, uppercase, numbers, and symbols. The estimated crack time is 1 month. A review states: "Good, using that password is like locking your front door and keeping the key in a safety deposit box."

The image displays three separate screenshots of a browser window running on a Windows operating system. Each screenshot shows the 'PasswordStrength-Meter' extension's interface for testing a password's security.

Screenshot 1:

- URL:** passwordmonster.com
- Title:** How Secure is Your Password?
- Password Entered:** 12345Jine6789ndra
- Rating:** Very Strong
- Character Breakdown:** 17 characters containing: Lower case, Upper case, Numbers, Symbols
- Crack Time:** 8 years
- Review:** Fantastic, using that password makes you as secure as Fort Knox.

Screenshot 2:

- URL:** passwordmonster.com
- Title:** How Secure is Your Password?
- Password Entered:** 12Ji345ne67ndra89
- Rating:** Very Strong
- Character Breakdown:** 17 characters containing: Lower case, Upper case, Numbers, Symbols
- Crack Time:** 90 billion years
- Review:** Fantastic, using that password makes you as secure as Fort Knox.

Screenshot 3:

- URL:** passwordmonster.com
- Title:** How Secure is Your Password?
- Placeholder Text:** Enter your password here