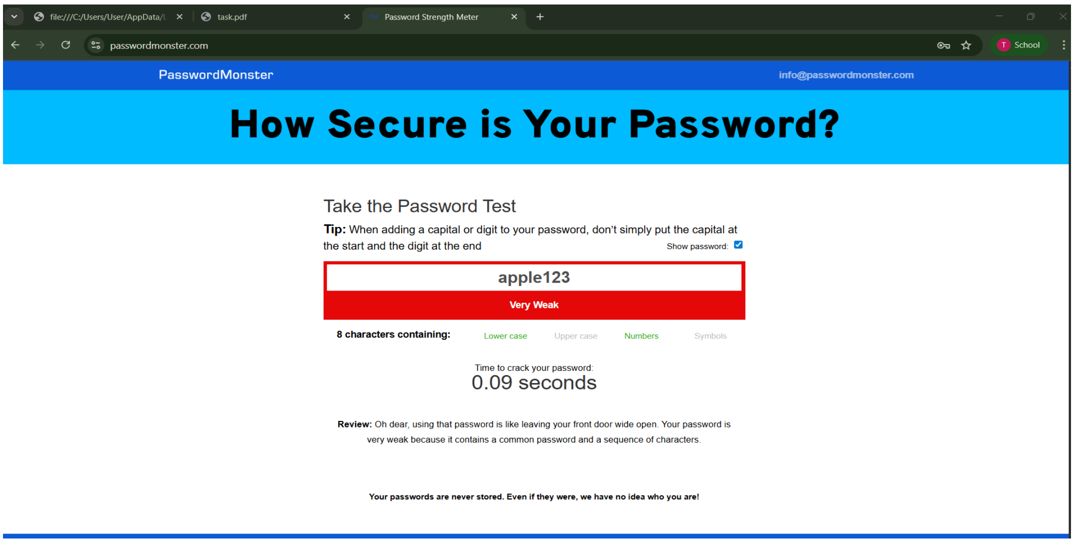
Password Strength Evaluation Report

This report evaluates multiple passwords of varying complexity using an online Password Strength Checker tool. The goal of this evaluation is to understand how password length, character variety, and complexity impact security.

1. Passwords Tested & Results

Password: apple123

Strength: Very Weak
Time to crack: 0.09 seconds



How Secure is Your Password?

Take the Password Test

Tip: When adding a capital or digit to your password, don't simply put the capital at the start and the digit at the end

Show password: ☑

apple123

Very Weak

8 characters containing: Lower case Upper case Numbers Symbols

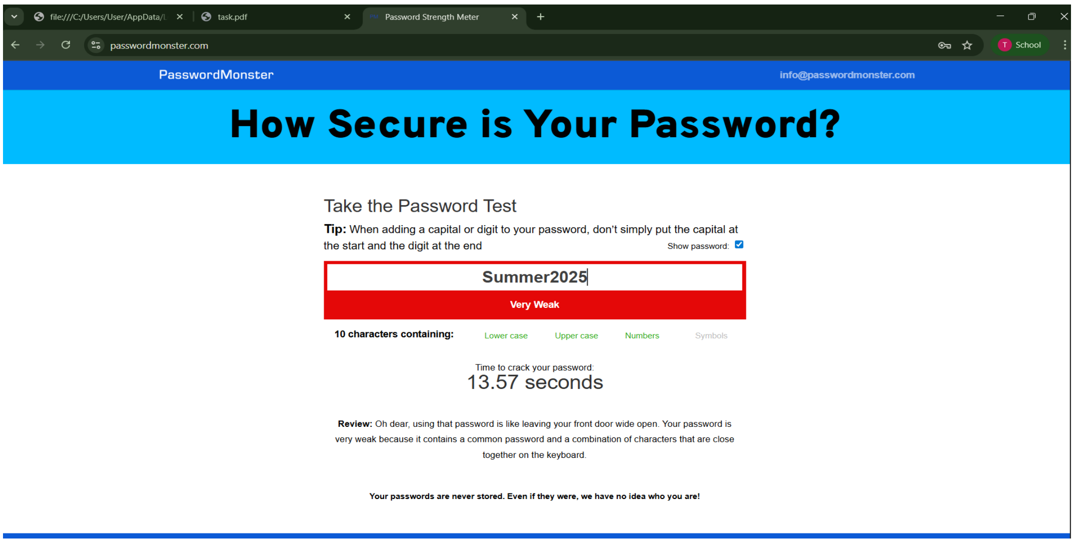
Time to crack your password:
0.09 seconds

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

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

Password: Summer2025

Strength: Very Weak
Time to crack: 13.57 seconds



How Secure is Your Password?

Take the Password Test

Tip: When adding a capital or digit to your password, don't simply put the capital at the start and the digit at the end

Show password: ☑

Summer2025

Very Weak

10 characters containing: Lower case Upper case Numbers Symbols

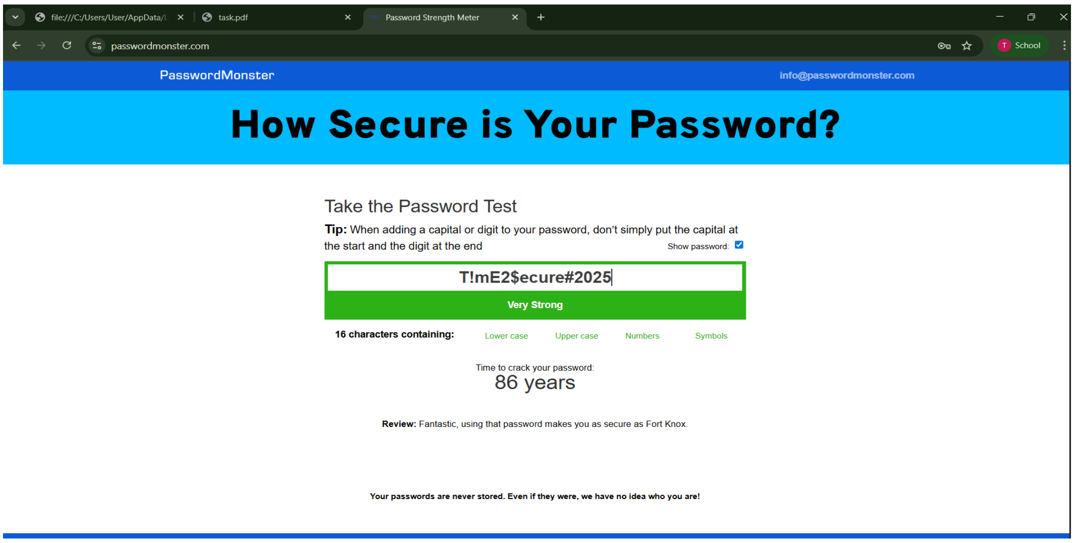
Time to crack your password:
13.57 seconds

Review: Oh dear, using that password is like leaving your front door wide open. Your password is very weak because it contains a common password and a combination of characters that are close together on the keyboard.

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

Password: T!mE2$ecure#2025

Strength: Very Strong
Time to crack: 86 years



How Secure is Your Password?

Take the Password Test

Tip: When adding a capital or digit to your password, don't simply put the capital at the start and the digit at the end

Show password: ☑

T!mE2$ecure#2025

Very Strong

16 characters containing: Lower case Upper case Numbers Symbols

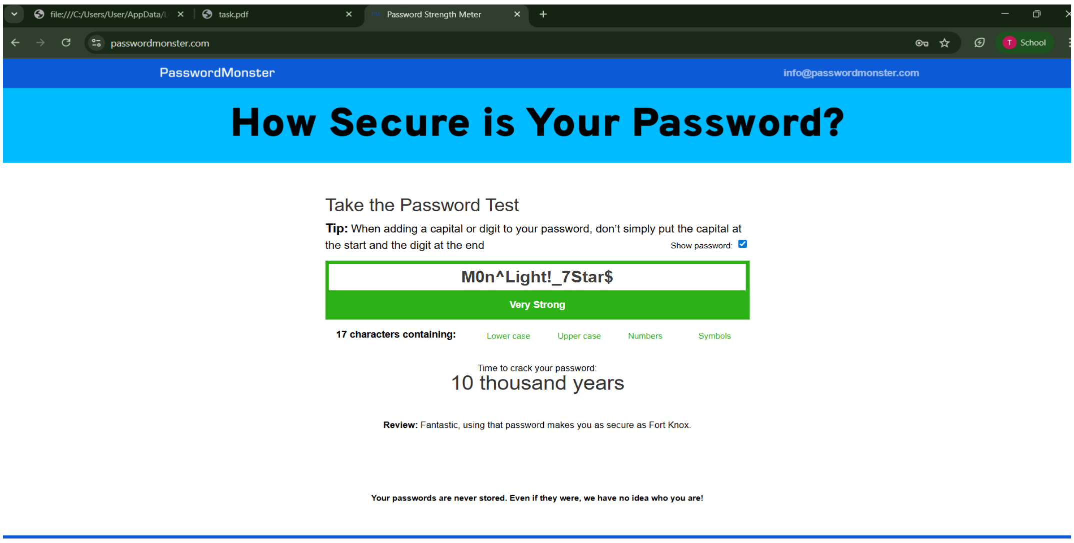
Time to crack your password:
86 years

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!

Password: M0n^Light!_7Star$

Strength: Very Strong
Time to crack: 10,000 years



PasswordMonster

info@passwordmonster.com

How Secure is Your Password?

Take the Password Test

Tip: When adding a capital or digit to your password, don't simply put the capital at the start and the digit at the end

Show password: ☑

M0n^Light!_7Star$

Very Strong

17 characters containing: Lower case Upper case Numbers Symbols

Time to crack your password:

10 thousand 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 & Feedback

- Simple and short passwords such as 'apple123' are cracked instantly.
- Slightly longer but predictable passwords like 'Summer2025' are still very weak.
- Complex passwords with mixed characters such as 'T!mE2$ecure#2025' greatly improve security.
- Highly complex and lengthy passwords like 'M0n^Light!_7Star$' are extremely secure and practically uncrackable.

3. Best Practices for Strong Passwords

1. Use at least 12–16 characters.
2. Mix uppercase, lowercase, numbers, and special characters.
3. Avoid dictionary words or predictable patterns.
4. Do not reuse passwords across accounts.
5. Use a password manager for securely storing complex passwords.

4. Tips Learned

- Length increases strength exponentially.
- Randomness is key: predictable words or sequences are weak.
- Special characters and mixed casing slow down brute force attacks significantly.

5. Common Password Attacks

- **Brute Force:** Tries all possible combinations until the correct password is found.
- **Dictionary Attack:** Uses a list of common words or known passwords.
- **Hybrid Attack:** Combines dictionary words with variations (e.g., adding numbers or symbols).
- **Phishing:** Tricks users into revealing passwords voluntarily.

6. Conclusion

Password complexity directly impacts security. Simple and short passwords are vulnerable to instant cracking, while long, complex, and unpredictable passwords can resist brute force and dictionary attacks for decades or even millennia. Users should adopt best practices to ensure strong password hygiene.