Create a Strong Password and Evaluate Its Strength

1. Password Generation (Varying Complexity)

Created multiple passwords with different complexities:

- hello123 (simple)
- Hello@123 (moderate)
- H3ll0_W@rld2025! (strong)
- P@55w0rd (commonly used, weak)
- G8#xL!9&zWq@5Y!m (very strong)

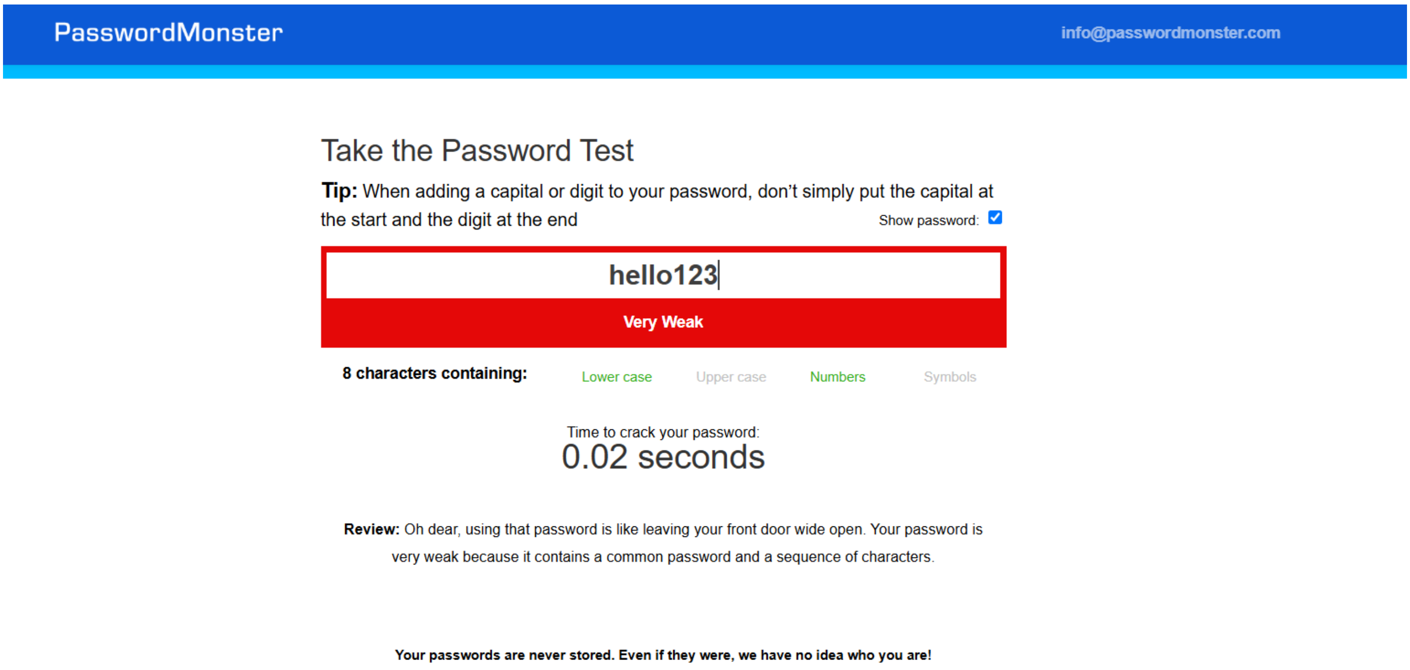
2. Password Components Used

- Uppercase: A–Z
- Lowercase: a–z
- Numbers: 0–9
- Symbols: @, #, $, %, etc.
- Length: Varied from 8 to 16+ characters

3. Password Strength Testing

Tested all passwords using online strength checkers like:

- Kaspersky Password Checker
- NordPass Strength Checker



PasswordMonster info@passwordmonster.com

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: ☑

hello123

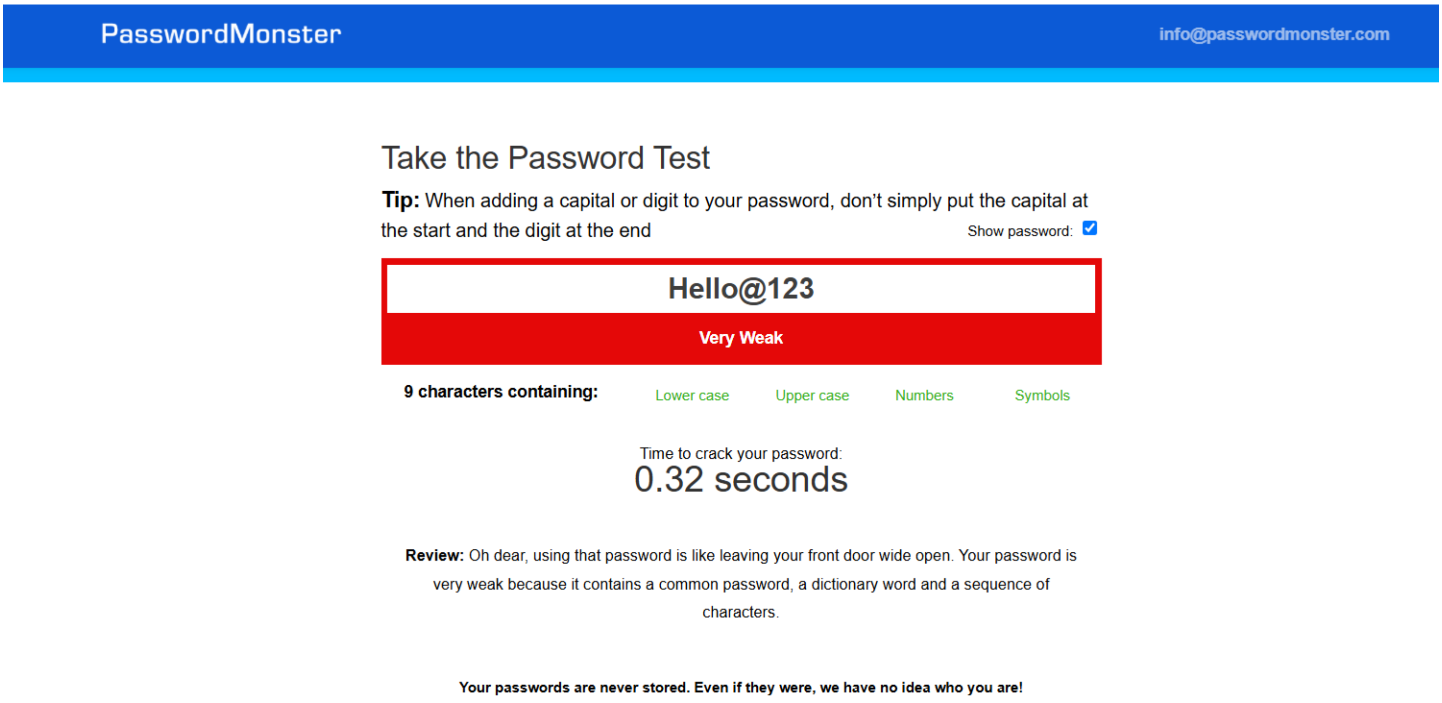
Very Weak

8 characters containing: Lower case Upper case Numbers Symbols

Time to crack your password:
0.02 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!



PasswordMonster info@passwordmonster.com

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: ☑

Hello@123

Very Weak

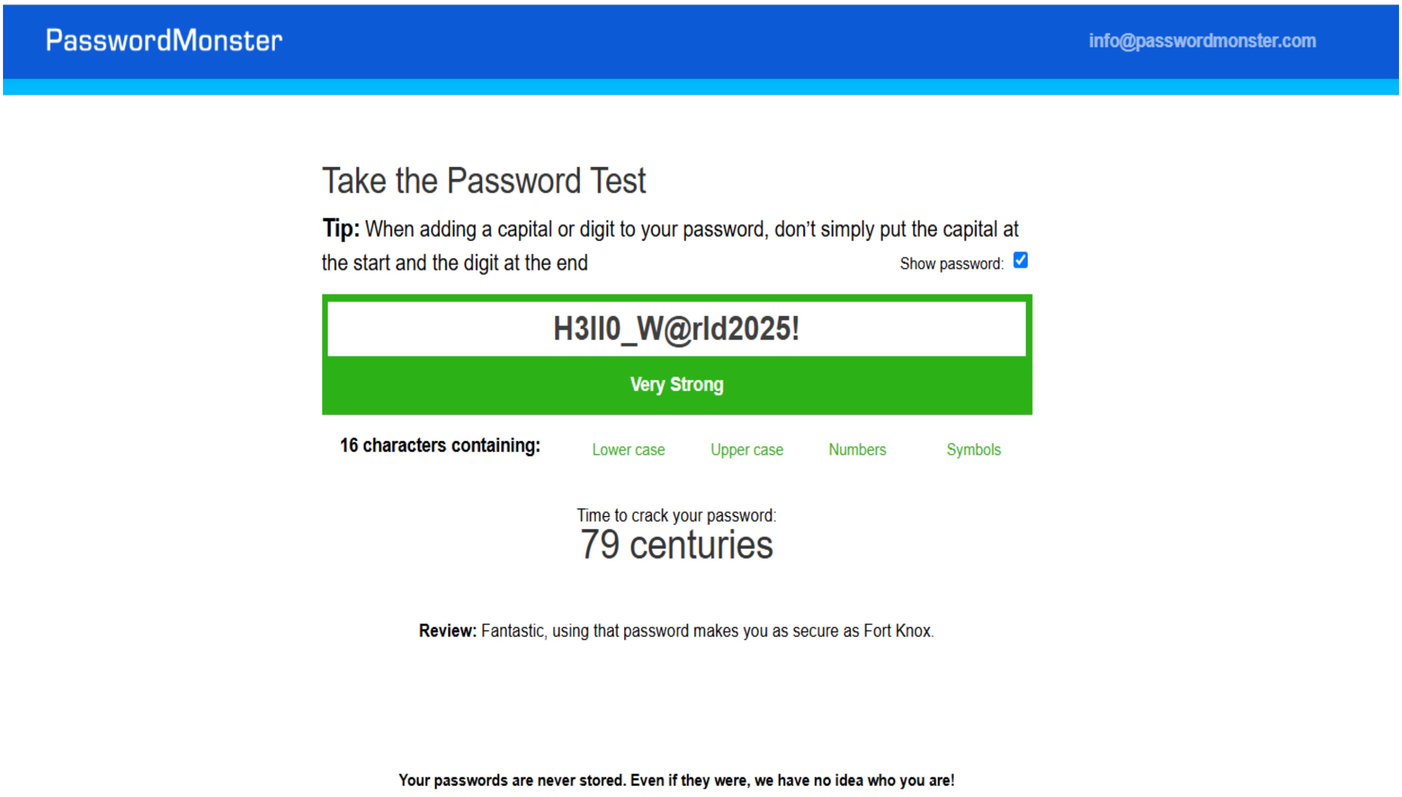
9 characters containing: Lower case Upper case Numbers Symbols

Time to crack your password:

0.32 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, a dictionary word and a sequence of characters.

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



PasswordMonster info@passwordmonster.com

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: ☑

H3ll0_W@rld2025!

Very Strong

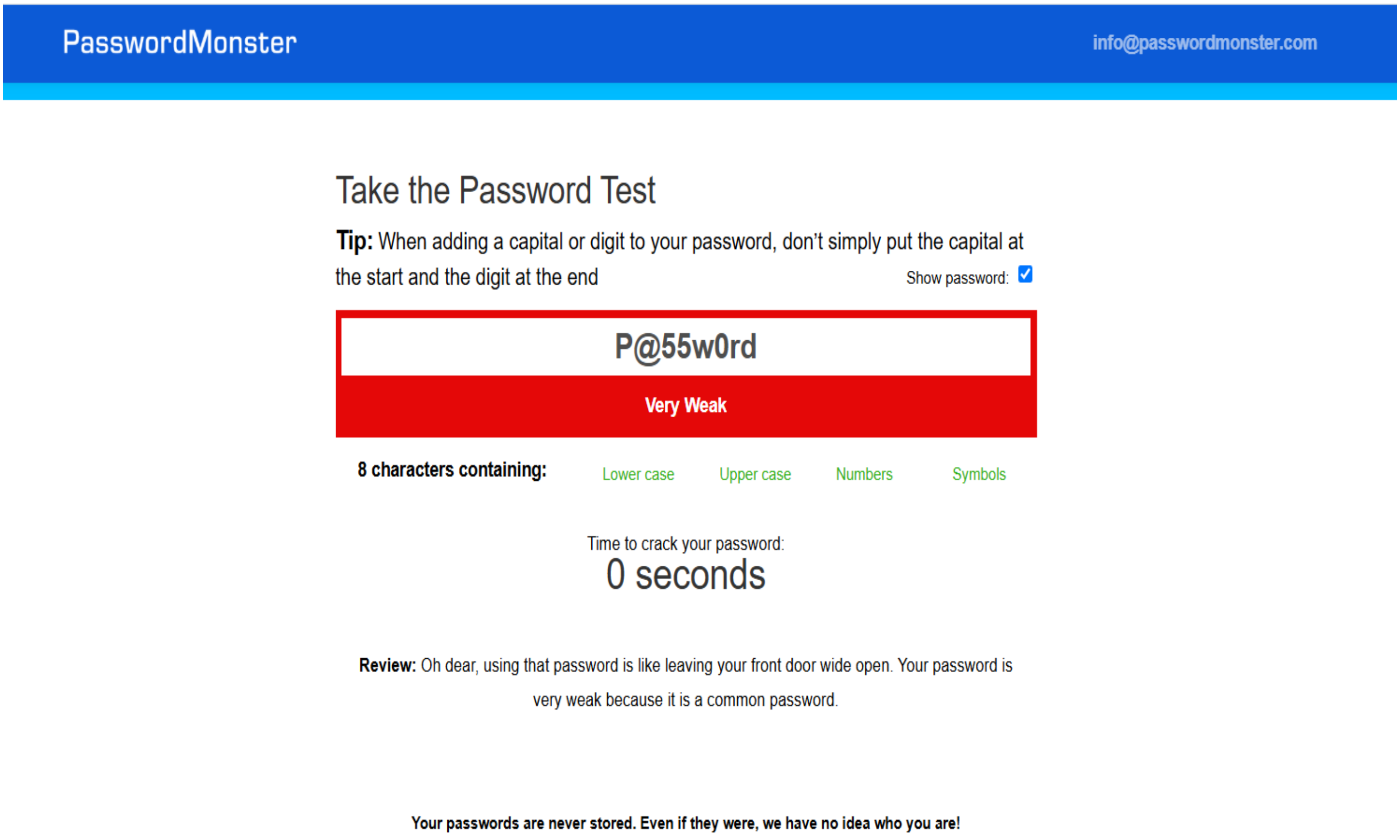
16 characters containing: Lower case Upper case Numbers Symbols

Time to crack your password:

79 centuries

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!



PasswordMonster info@passwordmonster.com

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: ☑

P@55w0rd

Very Weak

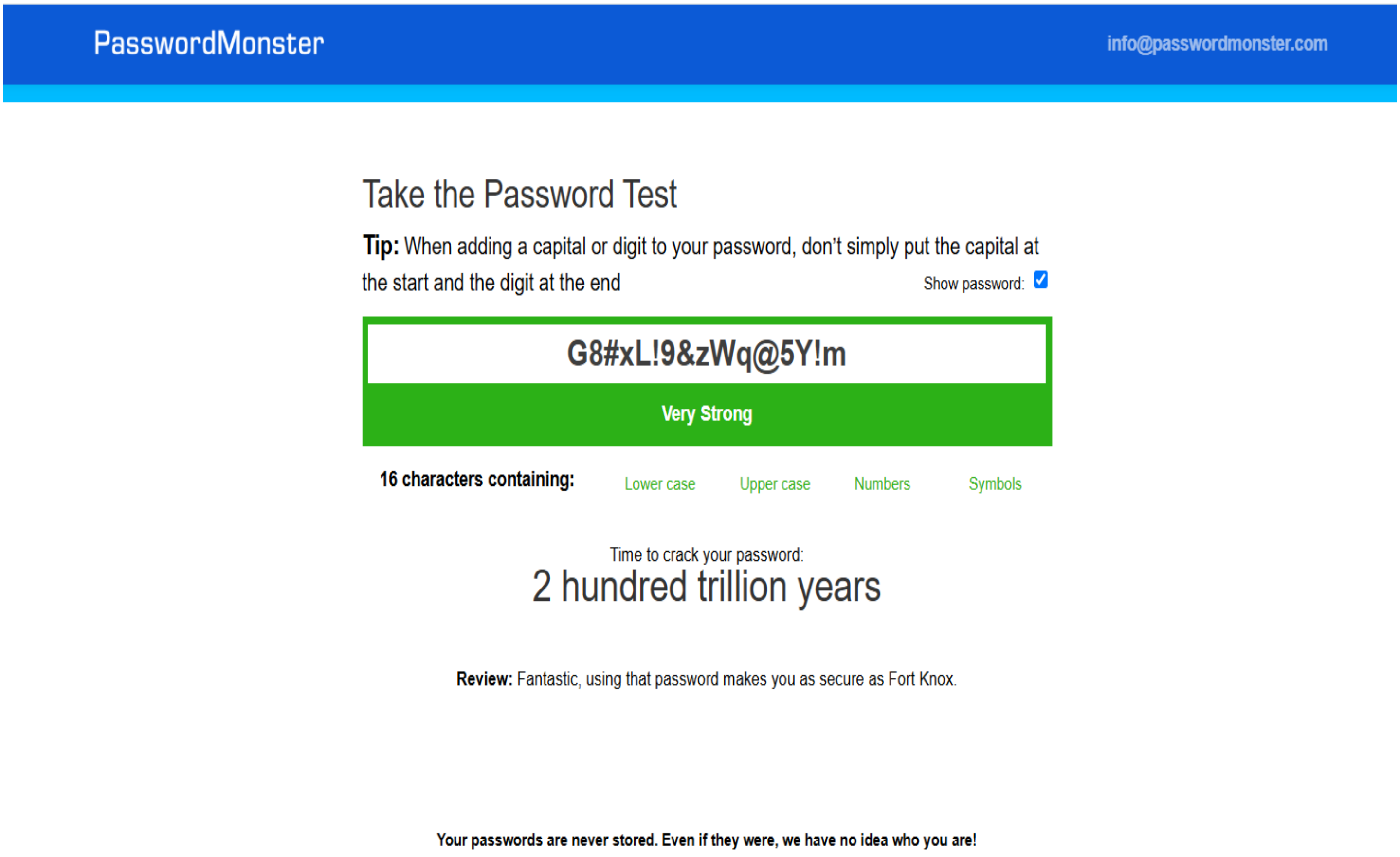
8 characters containing: Lower case Upper case Numbers Symbols

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!



PasswordMonster info@passwordmonster.com

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: ☑

G8#xL!9&zWq@5Y!m

Very Strong

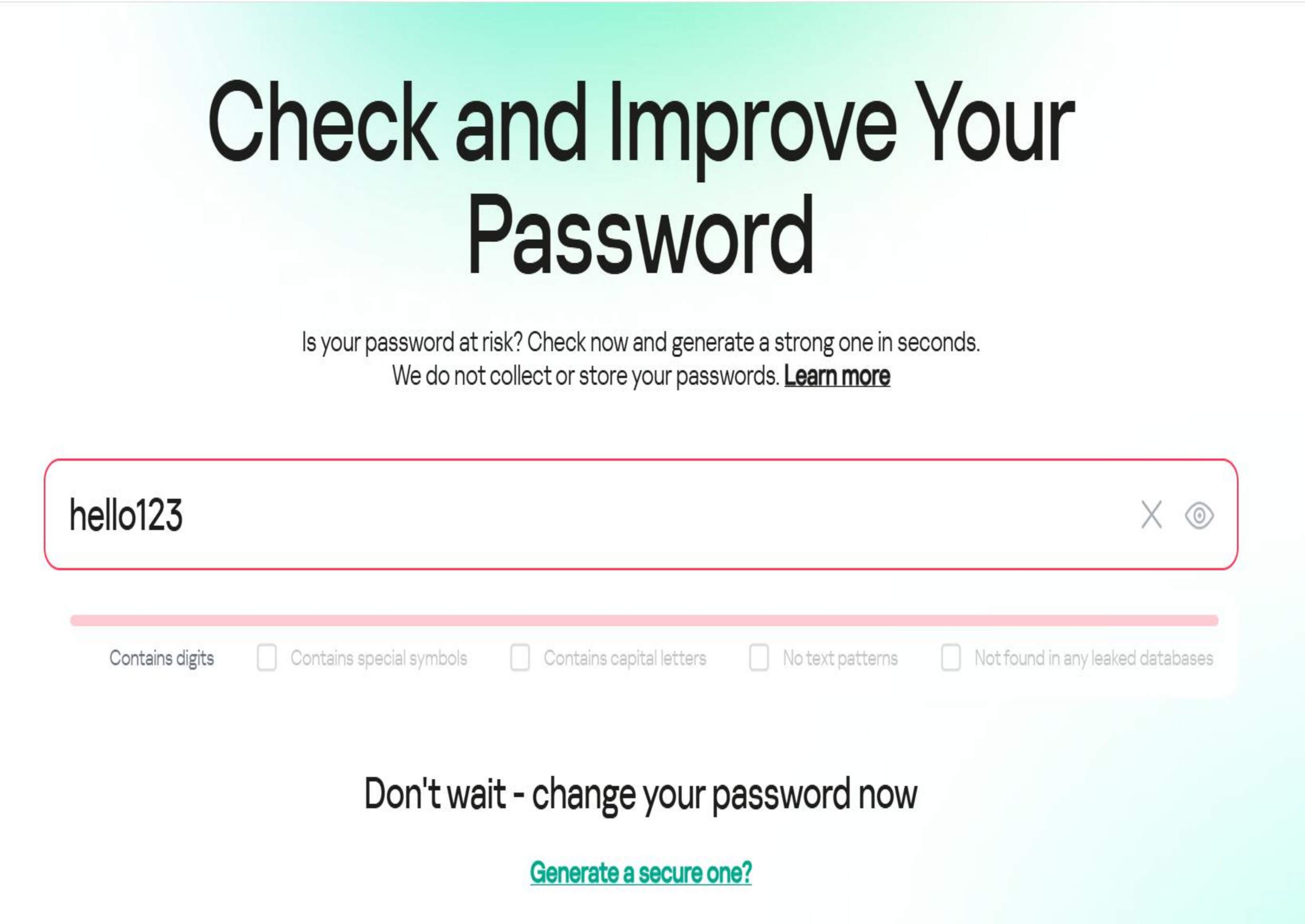
16 characters containing: Lower case Upper case Numbers Symbols

Time to crack your password:

2 hundred trillion 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!



Check and Improve Your Password

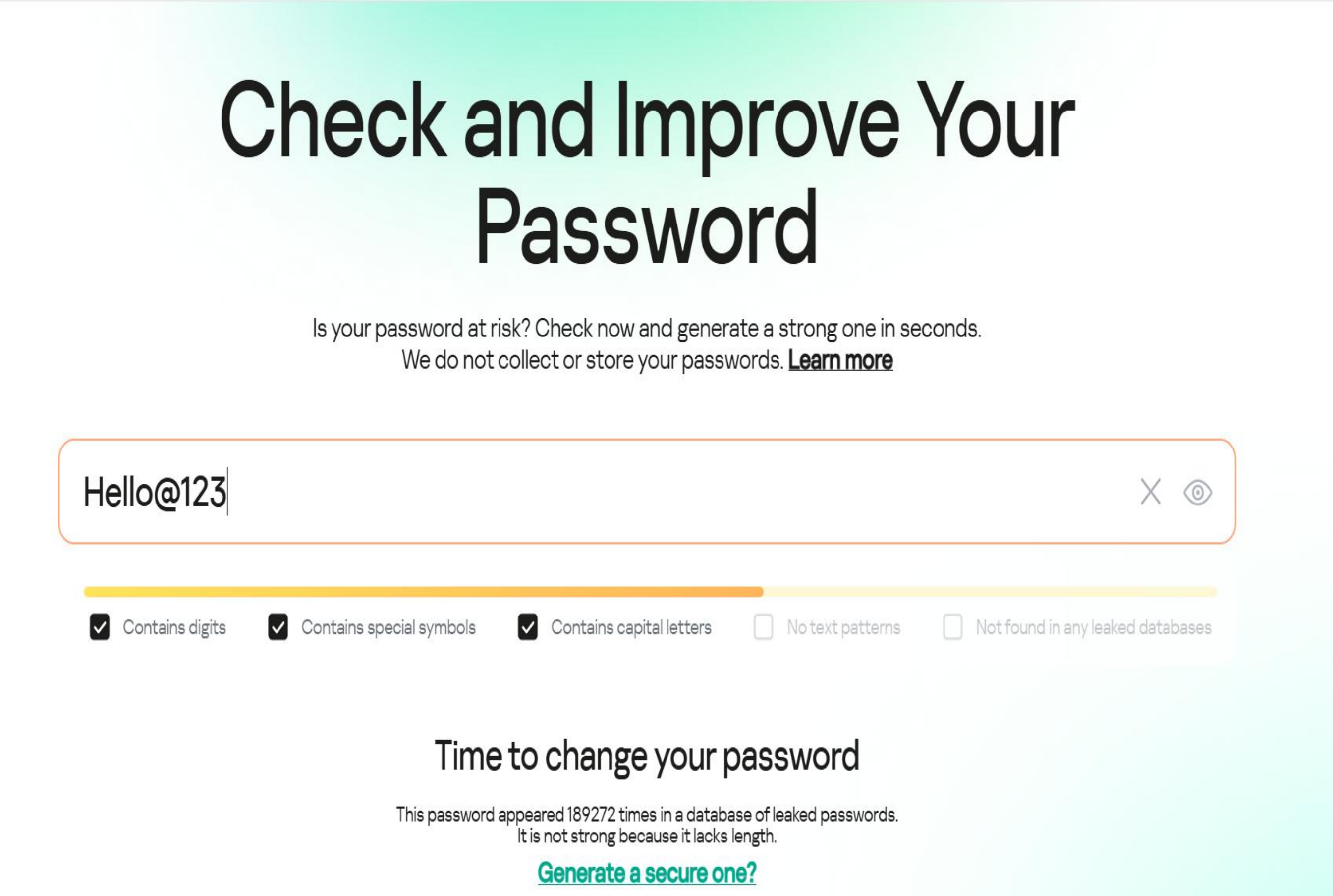
Is your password at risk? Check now and generate a strong one in seconds.
We do not collect or store your passwords. **Learn more**

hello123

Contains digits □ Contains special symbols □ Contains capital letters □ No text patterns □ Not found in any leaked databases

Don't wait - change your password now

Generate a secure one?



Check and Improve Your Password

Is your password at risk? Check now and generate a strong one in seconds.
We do not collect or store your passwords. **Learn more**

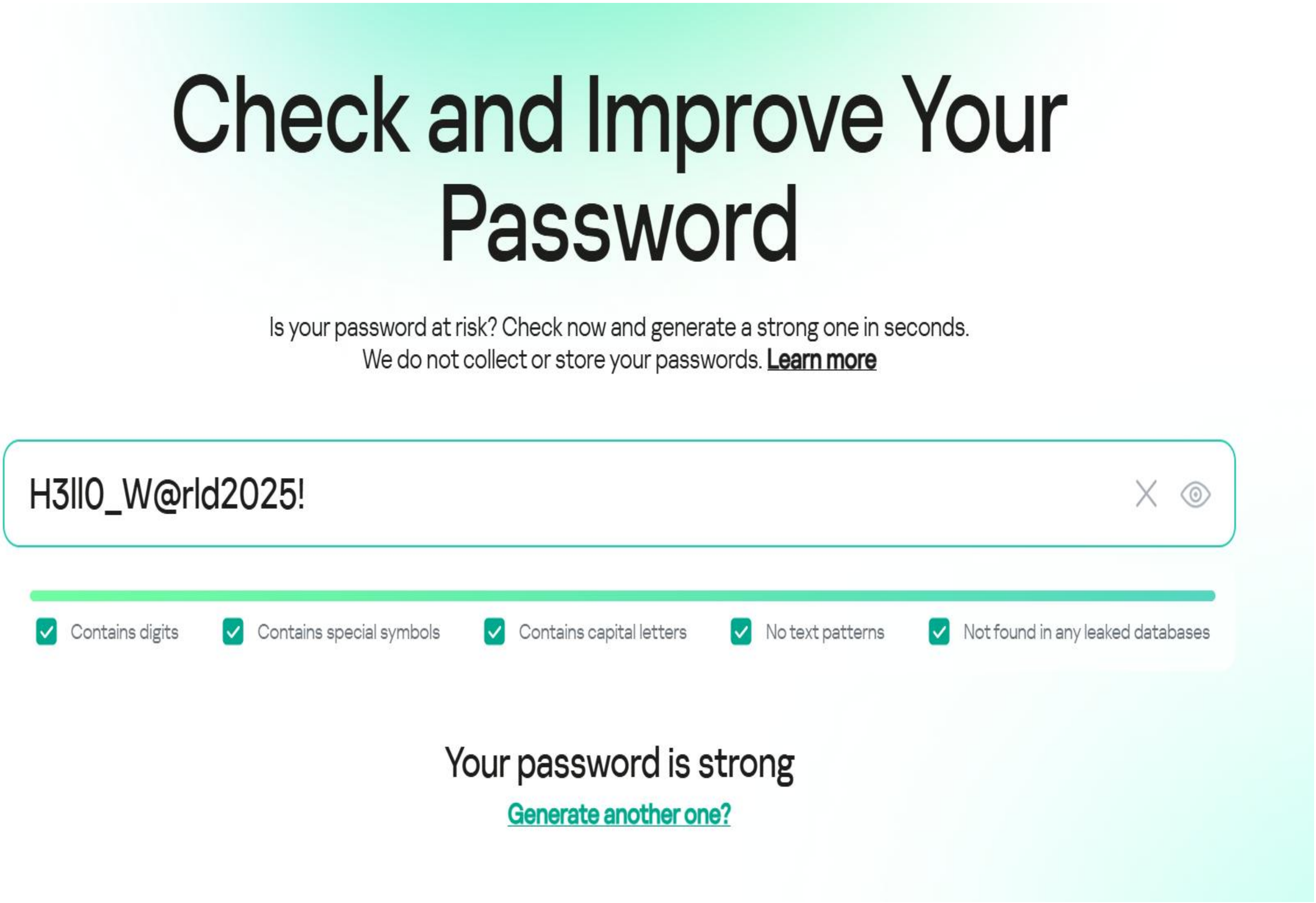
Hello@123

☑ Contains digits ☑ Contains special symbols ☑ Contains capital letters □ No text patterns □ Not found in any leaked databases

Time to change your password

This password appeared 189272 times in a database of leaked passwords.
It is not strong because it lacks length.

Generate a secure one?



Check and Improve Your Password

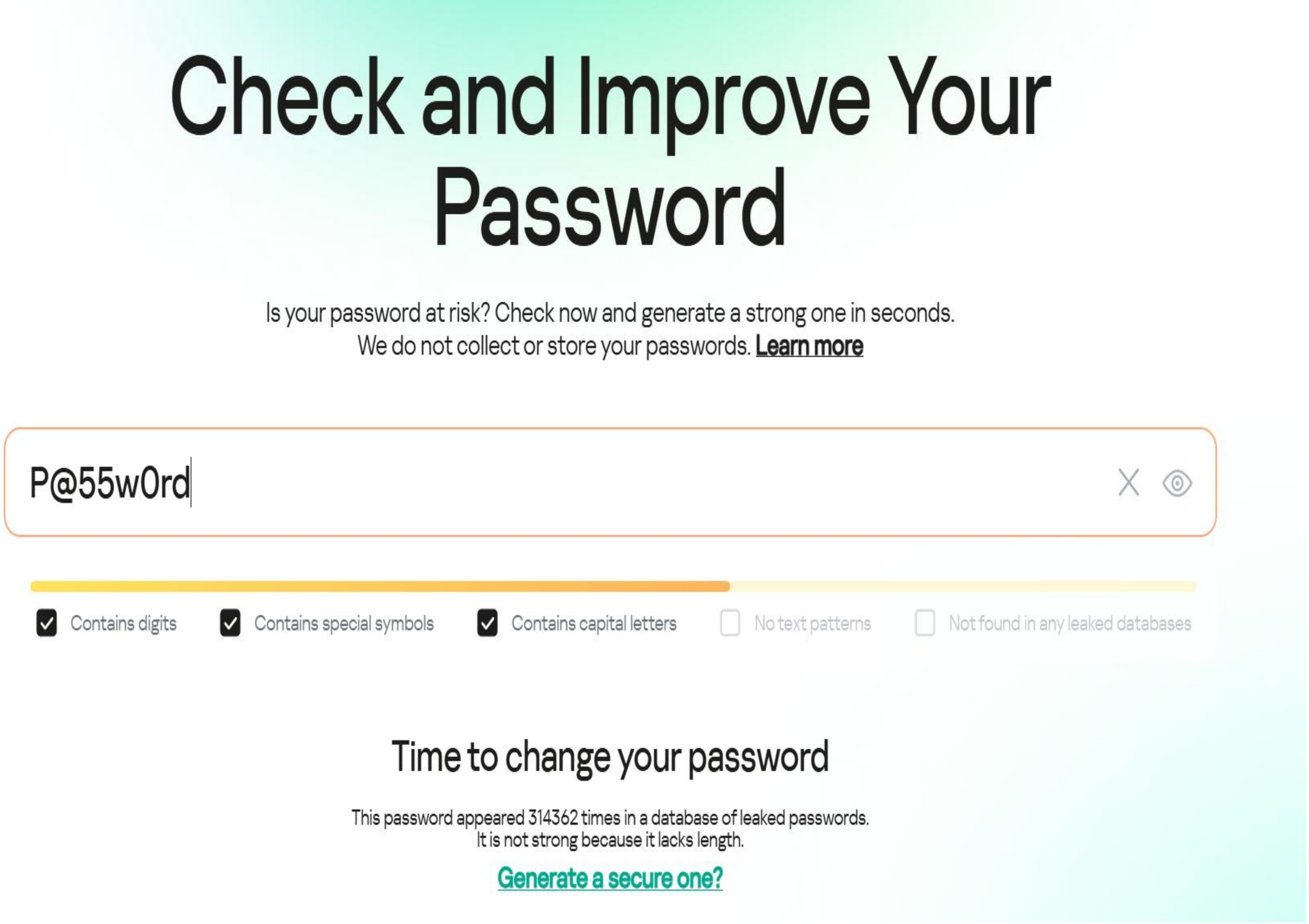
Is your password at risk? Check now and generate a strong one in seconds.
We do not collect or store your passwords. **Learn more**

H3ll0_W@rld2025!

☑ Contains digits ☑ Contains special symbols ☑ Contains capital letters ☑ No text patterns ☑ Not found in any leaked databases

Your password is strong

Generate another one?



Check and Improve Your Password

Is your password at risk? Check now and generate a strong one in seconds.
We do not collect or store your passwords. **Learn more**

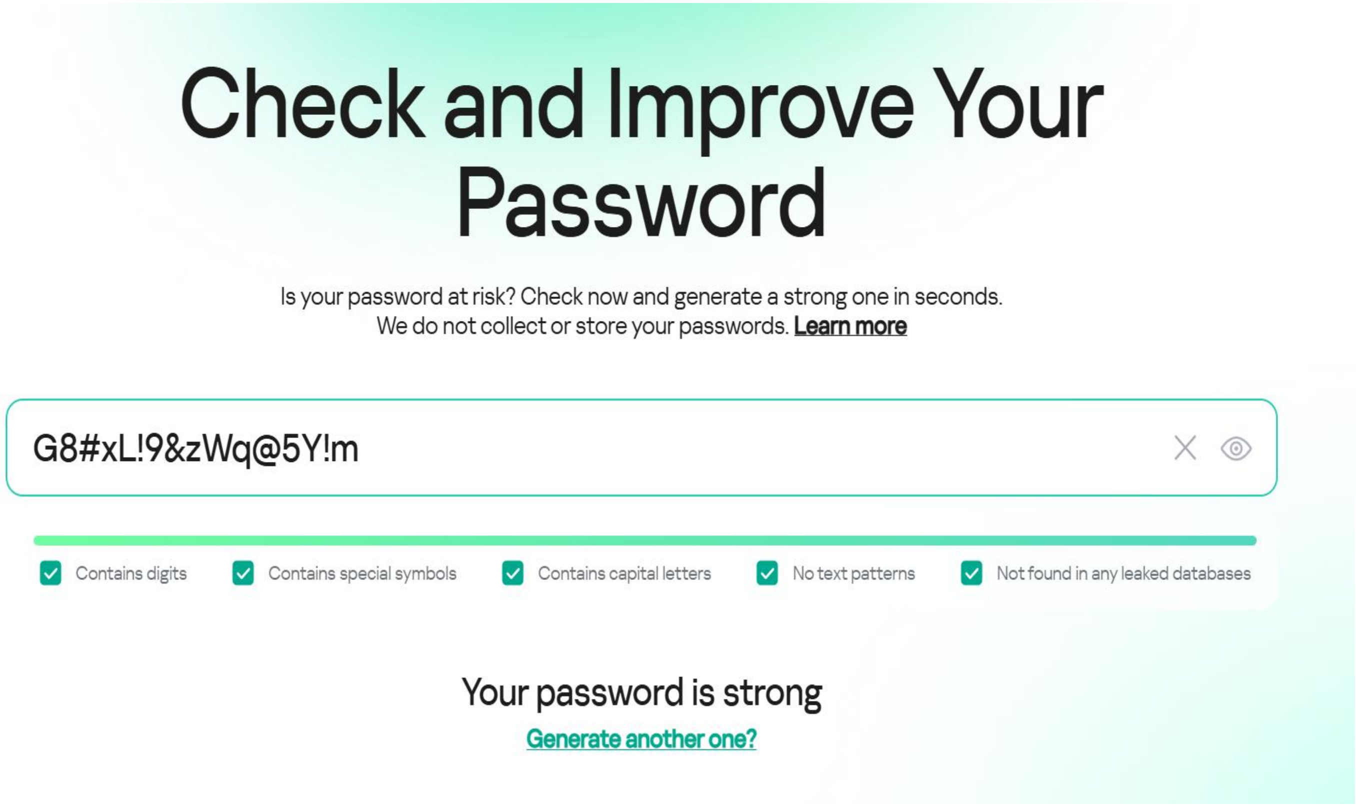
P@55w0rd

☑ Contains digits ☑ Contains special symbols ☑ Contains capital letters □ No text patterns □ Not found in any leaked databases

Time to change your password

This password appeared 314362 times in a database of leaked passwords.
It is not strong because it lacks length.

Generate a secure one?



Check and Improve Your Password

Is your password at risk? Check now and generate a strong one in seconds.
We do not collect or store your passwords. Learn more

G8#xL!9&zWq@5Y!m

☑ Contains digits ☑ Contains special symbols ☑ Contains capital letters ☑ No text patterns ☑ Not found in any leaked databases

Your password is strong

Generate another one?

4. Feedback and Scores

Password	Strength	Feedback
hello123	Weak	Too short, lacks symbols/uppercase
Hello@123	Medium	Could be longer
H3ll0_W@rld2025!	Strong	Good complexity and length
P@55w0rd	Weak	Commonly used, predictable
G8#xL!9&zWq@5Y!m	Very Strong	Excellent length and randomness

5. Best Practices Identified

- Use at least 12–16 characters
- Include uppercase, lowercase, numbers, and symbols
- Avoid common phrases or patterns
- Use unique passwords for every account
- Consider using a password manager to store complex passwords

6. Tips Learned

- Longer = stronger (exponentially harder to crack)
- Randomness is key: avoid dictionary words or keyboard patterns
- Mixing character types drastically increases strength
- Don't reuse passwords across sites

7. Common Password Attacks

- Brute Force: Tries all combinations — defeated by long/complex passwords
- Dictionary Attack: Uses common word lists — defeated by randomness
- Credential Stuffing: Reusing breached passwords — defeated by uniqueness
- Phishing: Social engineering — mitigated with cautious behavior, not password strength

8. Password Complexity vs Security

- Higher complexity exponentially increases time to crack passwords
- Simple passwords (even with length) are vulnerable to dictionary attacks
- Strong passwords protect against most automated attacks
- Human unpredictability + password manager = best combo for security

Summary: How Password Complexity Affects Security

- Password complexity significantly enhances security by making it much harder for attackers to guess or crack passwords using automated methods.
- Longer passwords take exponentially more time to brute-force.
- Mixed character types (uppercase, lowercase, numbers, symbols) greatly increase the number of possible combinations, making cracking attempts slower and less likely to succeed.
- Unpredictable and random passwords are resistant to dictionary and pattern-based attacks.
- Complex passwords reduce the risk of unauthorized access, especially when unique for every account.
- In short: the more complex and unique a password is, the more secure it becomes against modern cyberattacks.