Password Strength Evaluation Report

1. Objective

The objective of this task is to understand what makes a password strong, test different passwords using online strength checkers, analyze results, and derive best practices for creating secure passwords. This also involves understanding common password attacks and their relation to password complexity.

---

2. Passwords Created

Password	Description
`password123`	Simple and common
`Password2025`	Uses uppercase and numbers
`Pass@2025`	Includes a symbol
`S!mpl3_Ex@mpl3`	Complex, uses substitutions
`H@ppyD@ys_Are2025!`	Strong passphrase with symbols

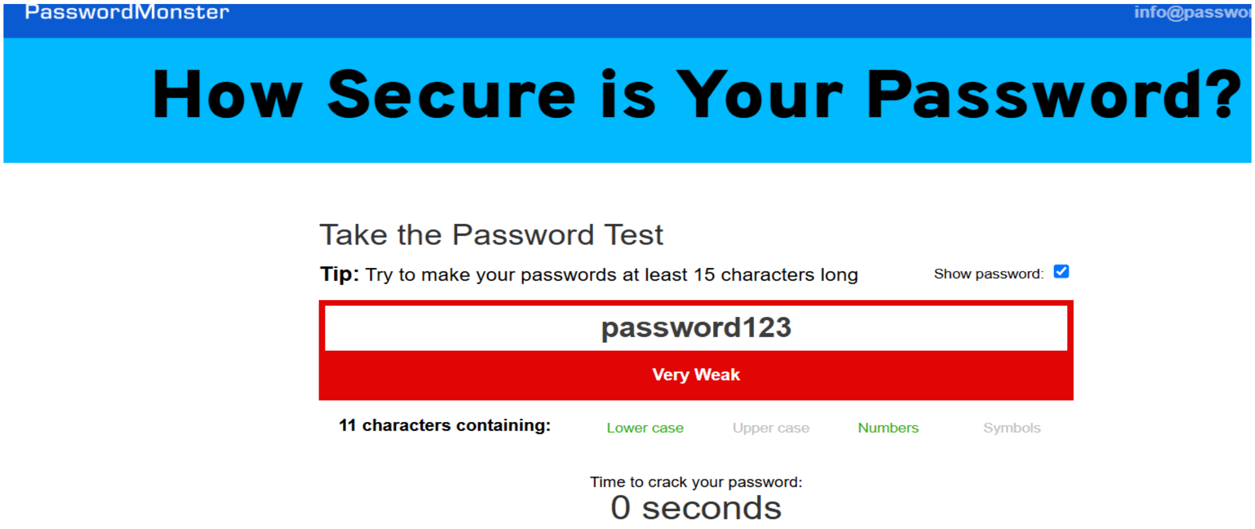
---

3. Tools Used

- https://www.passwordmonster.com/

---

4. Password Strength Results



PasswordMonster   info@passwo

How Secure is Your Password?

Take the Password Test

Tip: Try to make your passwords at least 15 characters long   Show password: ☑

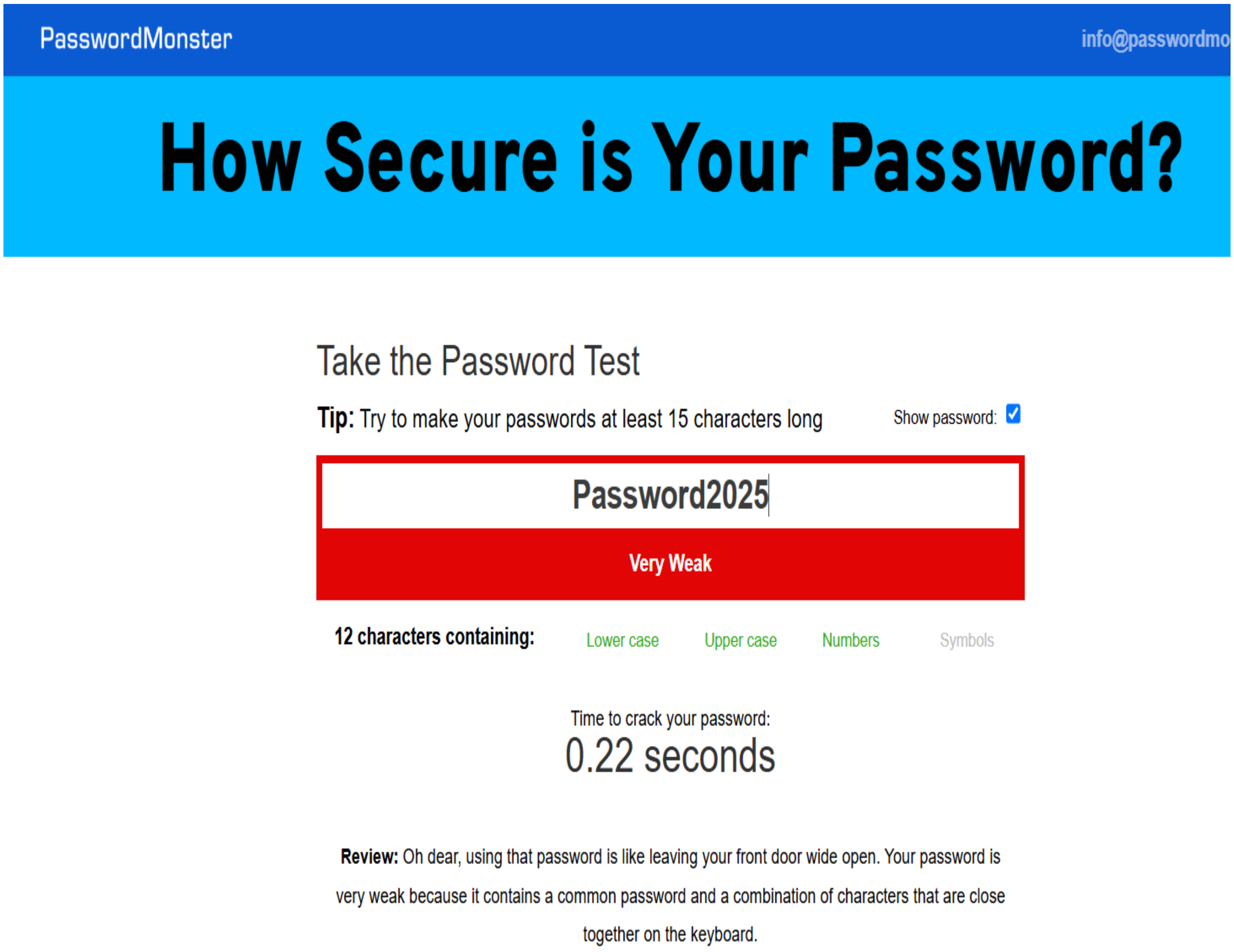
password123

Very Weak

11 characters containing: Lower case Upper case Numbers Symbols

Time to crack your password:

0 seconds



PasswordMonster   info@passwordmo

How Secure is Your Password?

Take the Password Test

Tip: Try to make your passwords at least 15 characters long   Show password: ☑

Password2025

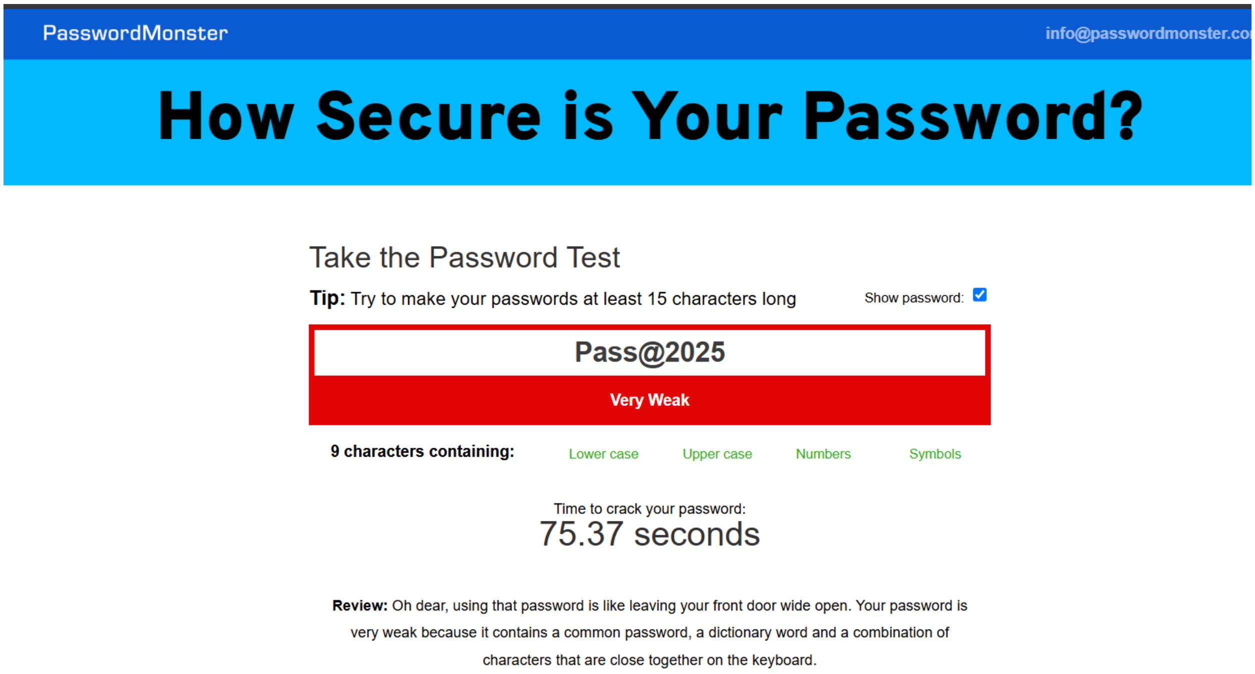
Very Weak

12 characters containing: Lower case Upper case Numbers Symbols

Time to crack your password:

0.22 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.



PasswordMonster

info@passwordmonster.co

How Secure is Your Password?

Take the Password Test

Tip: Try to make your passwords at least 15 characters long

Show password: ☑

Pass@2025

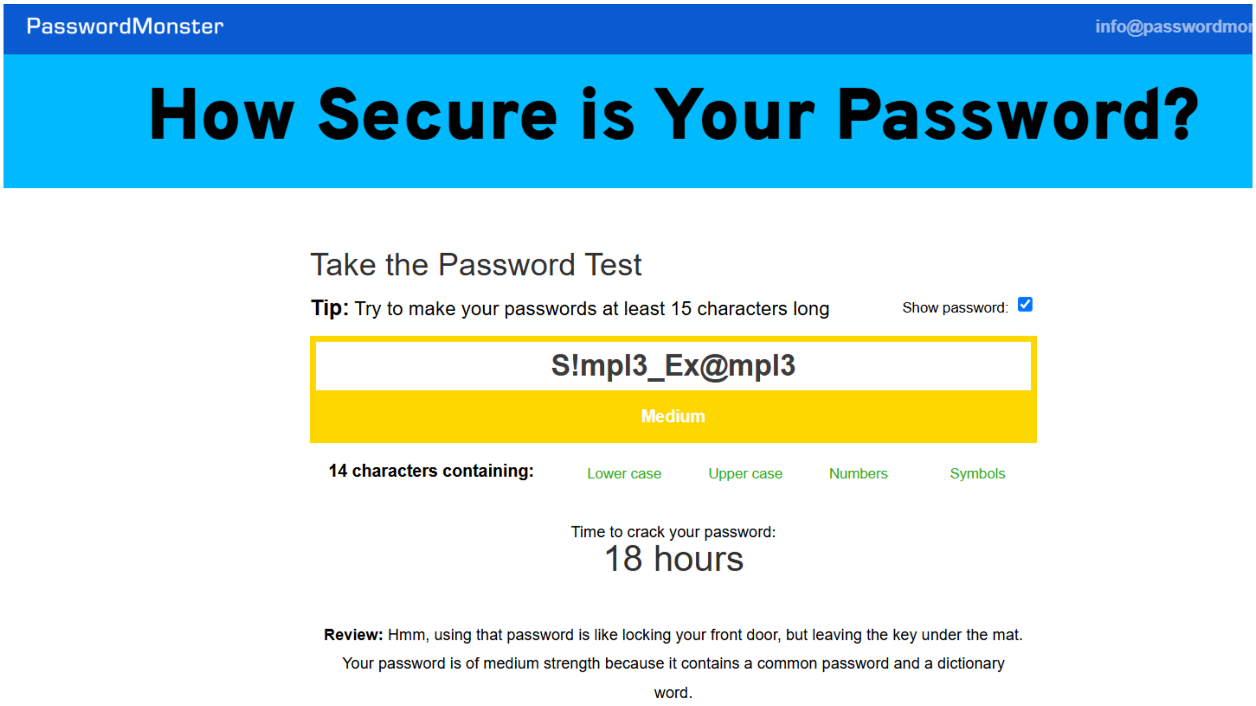
Very Weak

9 characters containing: Lower case Upper case Numbers Symbols

Time to crack your password:

75.37 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 combination of characters that are close together on the keyboard.



PasswordMonster

info@passwordmon

How Secure is Your Password?

Take the Password Test

Tip: Try to make your passwords at least 15 characters long

Show password: ☑

S!mpl3_Ex@mpl3

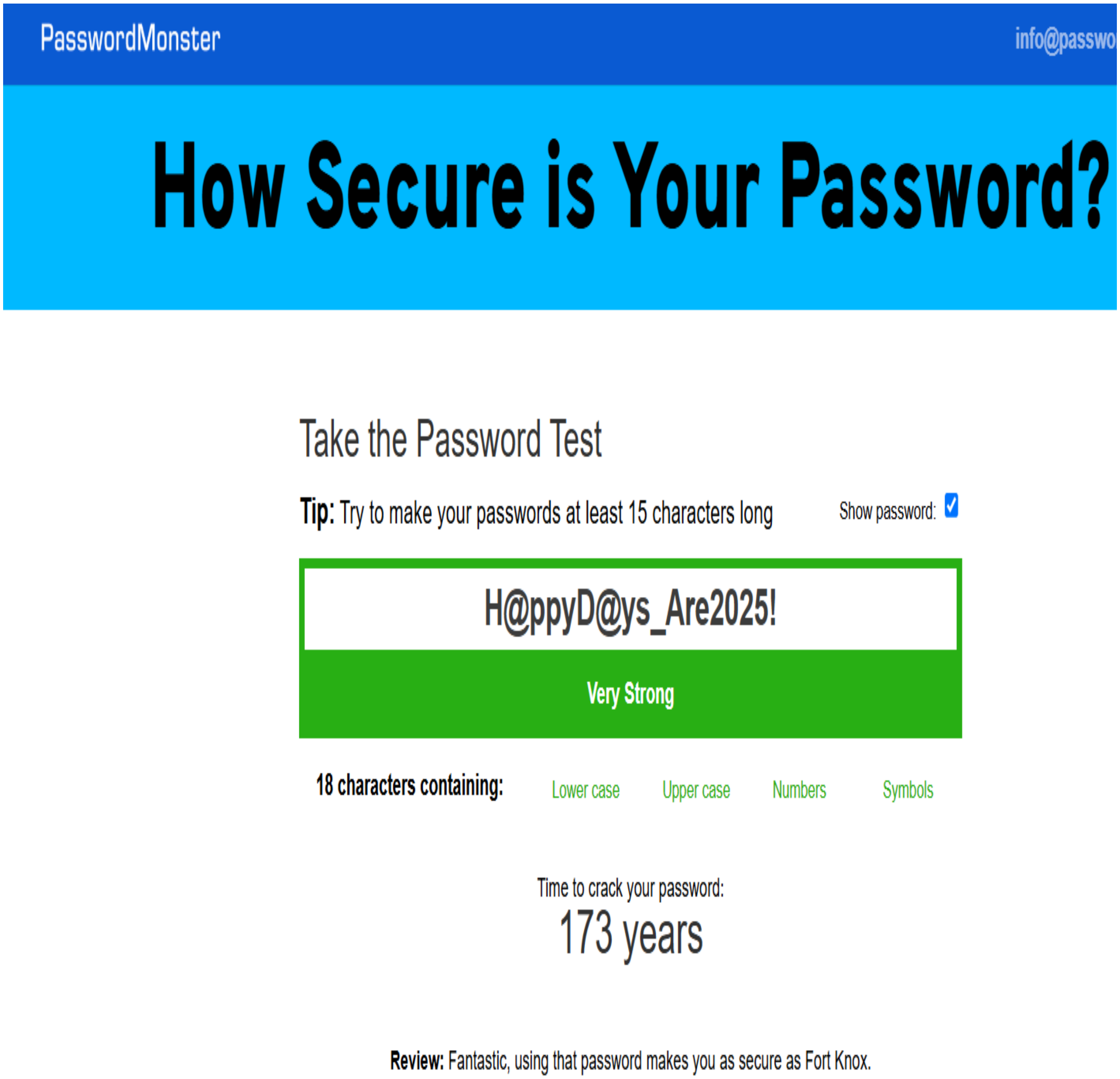
Medium

14 characters containing: Lower case Upper case Numbers Symbols

Time to crack your password:

18 hours

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 a common password and a dictionary word.



PasswordMonster

info@passwo

How Secure is Your Password?

Take the Password Test

Tip: Try to make your passwords at least 15 characters long

Show password: ☑

H@ppyD@ys_Are2025!

Very Strong

18 characters containing: Lower case Upper case Numbers Symbols

Time to crack your password:

173 years

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

5. Analysis of Results

- Simple and common passwords are instantly cracked.
- Adding **length**, **symbols**, and **unpredictable patterns** significantly increases security.
- The strongest password used a **passphrase** with multiple character types.
- Password strength is directly related to its **entropy—**randomness and unpredictabi

6. Tips and Best Practices Learned

- Use at least **12–16 characters**.
- Include **uppercase, lowercase, numbers, and symbols**.
- Avoid using dictionary words, names, or predictable sequences.
- Use **passphrases** (e.g., `Sun$hine_Rain!Cloud9`).
- Do not reuse passwords across different platforms.
- Use a **password manager** to generate and store complex passwords.
- Enable **multi-factor authentication (MFA)** wherever possible.

7. Common Password Attacks (Research Summary)

Attack Type	Description
Brute Force	Attempts all combinations; affected by length and complexity.
Dictionary Attack	Uses common words; weak passwords fall easily.

Credential Stuffing	Reuses stolen passwords from breaches.
Phishing	Tricks users into revealing passwords.

---

8. Password Complexity vs. Security

Password complexity increases the effort needed by attackers to crack passwords using brute force or dictionary methods. Longer and more diverse passwords reduce vulnerability. A strong password resists common attacks and increases the time required for successful guesses exponentially.

---

9. Conclusion

This task demonstrated the critical role of password strength in securing digital assets. By analyzing different passwords, using online tools, and understanding attack vectors, we conclude that strong passwords combined with multi-factor authentication and good password hygiene are essential to protect against modern cybersecurity threats.