TASK 6

1.Create multiple passwords with varying complexity

Password	Complexity
apple123	Low (common word + numbers)
Appl3!23	Medium (uppercase + number + symbol)
Y@8v$1pL!u3W	High (random, long, mixed)
Password1	Very Weak (common pattern)
C0mpl3x@#2025!	Strong (mixed case, symbols, long)

2.Use uppercase, lowercase, numbers, symbols, and length variations.

Element	Example Used
Uppercase	A, P, Y
Lowercase	p, l, e
Numbers	123, 2025
Symbols	@, !, #, $
Length	Ranges from 8 to 15+

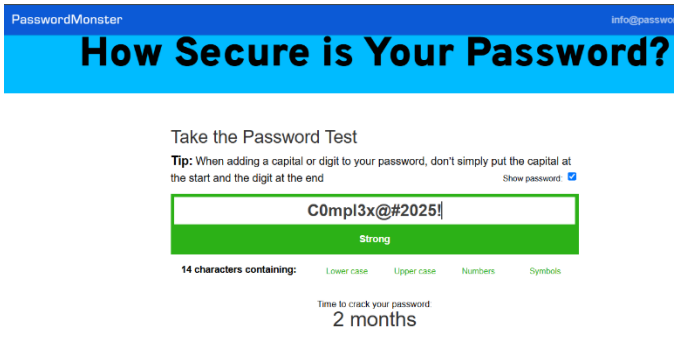
3.Test each password on password strength checker.


PasswordMonster
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


PasswordMonster
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:
Appl3!23
Very Weak
8 characters containing:
Lower case
Upper case
Numbers
Symbols
Time to crack your password:
49.42 seconds


PasswordMonster
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:
Y@8v$1pL!u3W
Very Strong
12 characters containing:
Lower case
Upper case
Numbers
Symbols
Time to crack your password:
9 million years


PasswordMonster
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:
Password1
Very Weak
9 characters containing:
Lower case
Upper case
Numbers
Symbols
Time to crack your password:
0 seconds


PasswordMonster
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:
C0mpl3x@#2025!
Strong
14 characters containing:
Lower case
Upper case
Numbers
Symbols
Time to crack your password:
2 months

4.Note scores and feedback from the tool.

1) It takes only 0.09 sec to crack the password - 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.

2)It takes only 49.42 sec. 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.

3) It takes 9 million years. Fantastic, using that password makes you as secure as Fort Knox.

4) It takes only 0 sec. 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 dictionary word.

5) It takes 2 months. Good, using that password is like locking your front door and keeping the key in a safety deposit box.

5.Identify best practices for creating strong passwords.

- Use at least **12–16 characters**
- Combine **upper/lowercase, numbers, symbols**

Avoid:

- Common words or names
- Simple substitutions (e.g., a → @, s → $)

- Reusing old passwords

6.Write down tips learned from the evaluation.

- Longer = stronger (exponentially harder to brute-force)
- "Password123!" is still weak (patterns are predictable)
- Use **passphrases** (e.g., Taco!Rain7!Mouse$) — easy to remember, hard to crack
- Password managers can help generate/store complex passwords

7.Research common password attacks (brute force, dictionary).

Attack Type	**Description**
Brute Force	Tries every possible combination
Dictionary Attack	Uses lists of common passwords/words
Credential Stuffing	Tries known passwords from data breaches
Phishing	Tricks user into revealing password
Keylogging	Records keystrokes to steal login data

8.Summarize how password complexity affects security.

- The **more complex** a password is (length + variation), the **exponentially harder** it becomes to crack.
- example:

- abc123 → cracked in seconds
- F4$kR@p9!zXv → years or more

 Password complexity protects against:

- **Brute force**: longer passwords = more combinations
- **Dictionary attacks**: randomness beats predictability