Task 6 – Create a Strong Password and Evaluate Its Strength

Objective

To create strong passwords, evaluate their strength using free online tools, and identify security weaknesses and best practices related to password creation.

Tools Used

- Password Strength Checkers:
  - passwordmeter.com
  - howsecureismypassword.net
- Operating System: Windows
- Browser: Google Chrome

Steps Performed

1. Created Passwords
   Generated five different passwords with increasing complexity using combinations of uppercase, lowercase, numbers, symbols, and length variations.
2. Tested Passwords on Password Strength Checkers
   Each password was evaluated using:
   - PasswordMeter: For score and complexity.
   - HowSecureIsMyPassword: For estimated time to crack by a computer.
3. Collected Results and Feedback
   Recorded the score, complexity, and cracking time, and noted feedback on weak elements like repetition, sequence, or lack of symbols.
4. Analyzed Password Best Practices
   Studied password construction techniques and common attack methods like brute force and dictionary attacks.
5. Documented Tips and Observations
   Summarized findings to create recommendations for strong passwords.

Passwords Evaluated

Password	Score	Crack Time	Complexity	Tool Feedback Summary
Password123	75%	3 weeks	Strong	No symbols, common pattern, easily guessed
P@ssw0rd!	82%	41 years	Very Strong	Good use of symbol and case mix, short length
Myp@ssw0rd2025!	100%	15 billion years	Very Strong	Excellent length, full mix of character types
#S3cur3L1f3*	100%	34 thousand years	Very Strong	High entropy, well-constructed but slightly short
T1g3r$h@dow!2025	100%	1 trillion years	Very Strong	Long, highly complex, no common sequences or words

Concepts Identified

Concept	Description
Password Strength	Measured by complexity, length, and randomness
Brute Force Attack	Tries every possible combination until the password is found
Dictionary Attack	Uses a database of commonly used words/passwords to guess login credentials
Passphrases	Multiple random or meaningful words combined (e.g., CorrectHorseBatteryStaple)
Password Managers	Applications that generate and store secure, unique passwords
Multi-Factor Authentication (MFA)	Adds another verification layer like OTP or biometrics

Key Learnings

- Longer passwords with mixed characters significantly increase strength.
- Simple patterns and dictionary words make passwords highly vulnerable.
- Password managers and MFA can mitigate risks even if a password is leaked.
- Passwords that are over 15 characters with symbols and case variety are exponentially harder to crack.

Outcome

Successfully created and tested five different passwords.
Gained insight into what makes a password secure and understood how attackers exploit weak ones.
Tools confirmed that well-crafted passwords can resist even advanced attacks for billions of years.