**TASK 6: Create a strong Password and evaluate its strength.**

1. **Create multiple passwords with varying complexity.**

* P@ssword12
* Swift@6767
* God!sgre@t
* Just!magine
* Home@123
* An0nymous89
* Crack!t@489

1. Test each password in password strength checker.
2. Scores and feedback from the tool.
   * P@ssword12 – weak, 11.43 Minutes
   * Swift@6767 - very strong – 3 years
   * God!sgre@t - Medium- 10 hours
   * Just!magine - Medium- 10 hours
   * Home@123 – very weak – 1.06 seconds
   * An0nymous89 - strong – 3 years
   * Crack!t@489 - very strong – 8 years
3. Identify best practices for creating strong passwords.

**1. Use Long Passwords**

* Minimum: **12–16 characters**
* Longer passwords are harder to crack via brute-force attacks.

**2. Include a Mix of Characters**

* Use **uppercase (A–Z)**, **lowercase (a–z)**, **numbers (0–9)**, and **special characters** (e.g., ! @ # $ % ^ & \*).
* Example: T3ch!SecuR3#2025

**3. Avoid Common Words or Patterns**

* Never use:
  + "password", "123456", "qwerty"
  + Birthdays, names, or keyboard patterns (e.g., "asdf")

**4. Use Passphrases**

* Combine unrelated words to create a memorable but strong phrase.
* Example: Sunlight\_Tiger!Ice92

**5. Never Reuse Passwords**

* Each account should have a **unique password** to prevent **credential stuffing attacks**.

1. Common password attacks:

* Bruteforce: The attacker tries every possible combination until the correct password is found.
* Dictionary attack: The attacker uses a list of common passwords or words (like from a dictionary) to guess the password.
* Credential Stuffing: Stolen credentials from one website are reused on other sites (since many people reuse passwords).
* Phishing: The attacker tricks you into revealing your password via fake emails or websites.

1. Summary of how password complexity affects security:

* Increases Resistance to Attacks
* Slows Down Brute Force and Dictionary Attacks
* Defeats Common Word-Based Guesses