Create a Strong Password and Evaluate Its Strength.

Objective: Understand what makes a password strong and test it against password strength tools.

Tools: Online free password strength checkers (e.g., passwordmeter.com).

Deliverables: Report showing password strength results and explanation

STEP 01- Create multiple passwords with varying complexity.

STEP 02 - Use uppercase, lowercase, numbers, symbols, and length variations

- password@123 – Very weak
- QWERTY@12345- Weak
- Welcome#2025- Fair
- KJGhdbn@#kjhfj- Strong
- !xY92$@wKe#l8rPqZ – Strong
- Z3nTh$Yolo@42#Time – Strong
- Pneumonoultramicroscopicsilicovolcanoconiosis123! - Very Strong

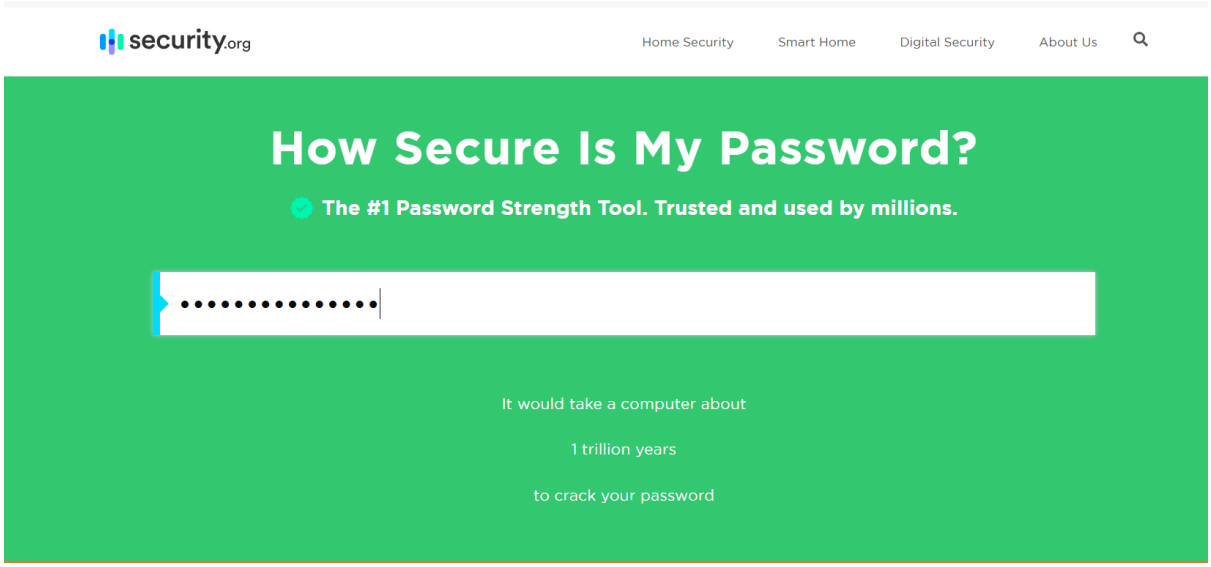
STEP 03 - Test each password on password strength checker.

LINK - https://howsecureismypassword.net/

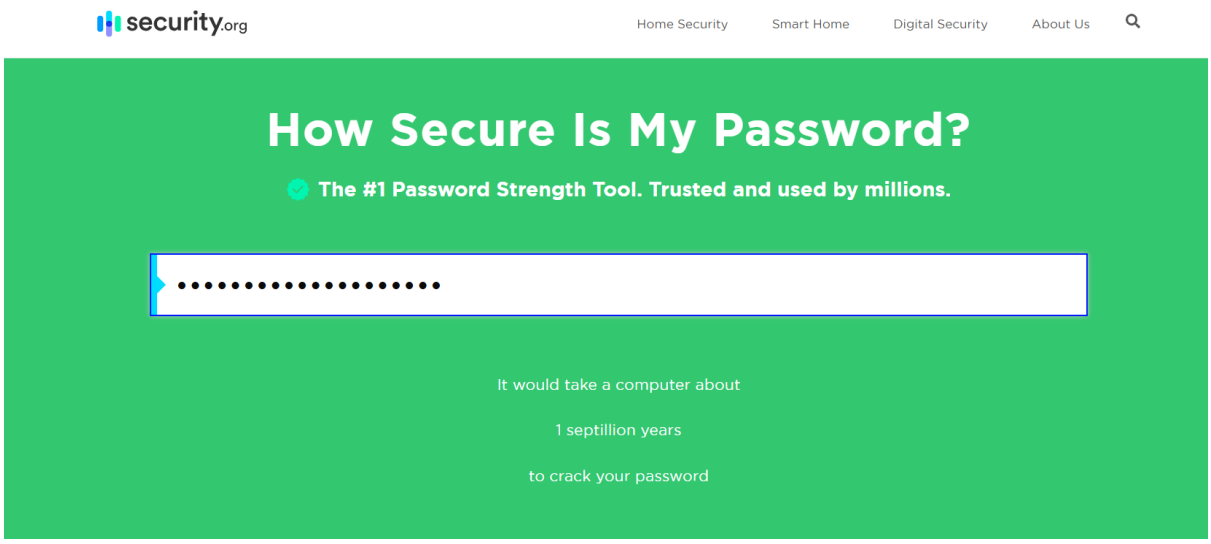
LINK - https://www.security.org/how-secure-is-my-password/

STEP 04 - Note scores and feedback from the tool

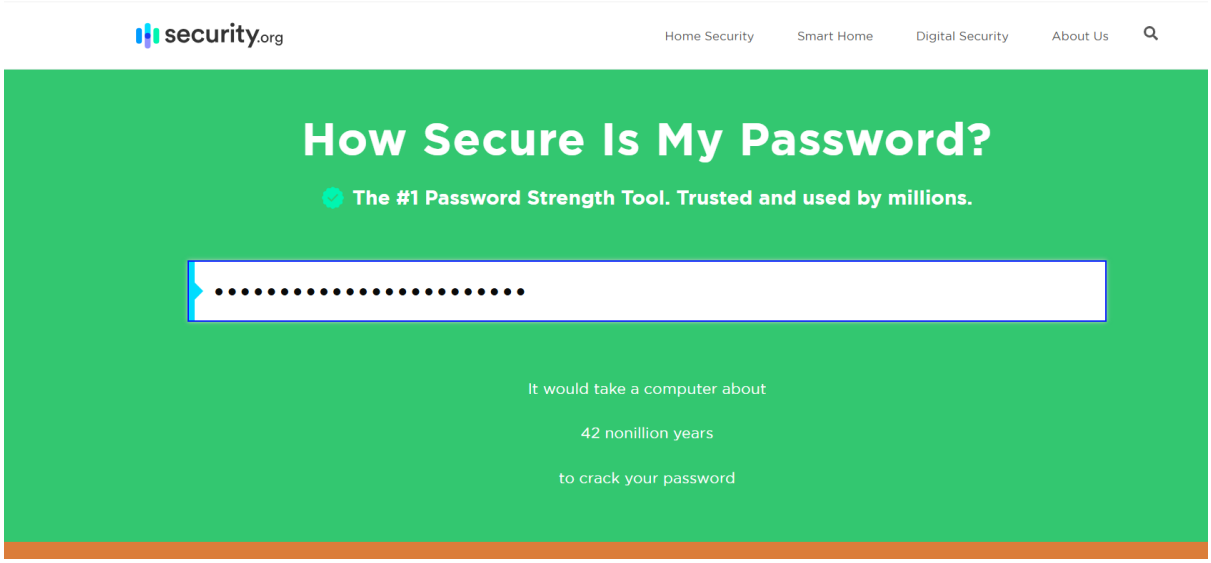
- password@123 – Very weak



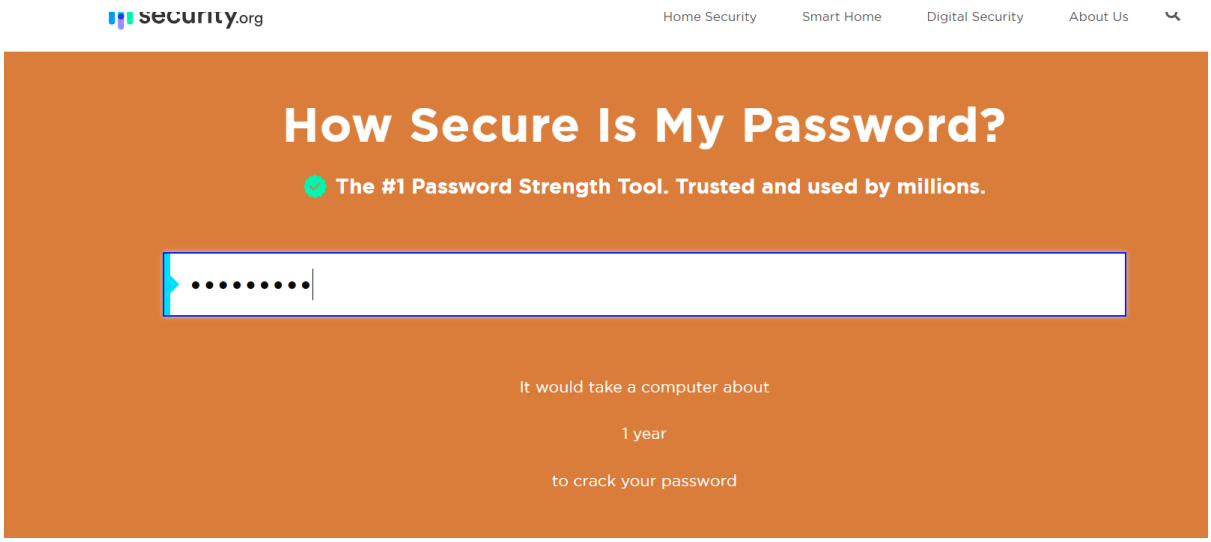
- QWERTY@12345- Weak



- KJGhdbn@#kjhfj- Strong



- Welcome#2025- Fair



STEP 05 - Identify best practices for creating strong passwords.

- Use **12+ characters** whenever possible.
- Combine **uppercase, lowercase, numbers, and special characters**.
- Avoid **dictionary words** and common substitutions (P@ssw0rd is predictable).
- Use a **passphrase** (e.g., Sunny$Horse!Jumps22) for both strength and memorability.
- **Do not reuse passwords** across multiple sites.

STEP 06 -Write down tips learned from the evaluation

Tips Learned from Evaluation

1. Longer = Stronger. Every extra character makes brute-force harder.
2. Randomness defeats dictionary attacks.
3. Substituting symbols in common words (P@ssword1) is not as safe as believed.
4. Password managers can help generate and store complex passwords securely.
5. Two-Factor Authentication (2FA) is a must for sensitive accounts.

STEP 07 - Research common password attacks (brute force, dictionary).

Common Password Attacks

- **Brute Force Attack**: Tries every possible combination.
- **Dictionary Attack**: Uses a list of common passwords and words.
- **Credential Stuffing**: Reuses leaked credentials from other sites.
- **Phishing**: Tricks user into revealing password.

STEP 08 - Summarize how password complexity affects security.

- Password complexity greatly increases security by making it harder for attackers to crack passwords using brute-force or dictionary attacks.
- Simple passwords (e.g., 123456, password) are highly vulnerable and can be guessed in seconds.
- Strong passwords with randomness, length, and mixed character types significantly reduce the risk of compromise.