Task 6 Report

Password Strength Evaluation

1. Objective

The purpose of this task is to understand what makes a password strong, evaluate several candidate passwords using industry standard online tools, and reflect on how length, complexity, and unpredictability improve resistance to common cracking techniques such as brute-force and dictionary attacks.

2. Screenshot Based Evaluation

Password Complexity (Caption)	Time to Crack
Very Weak	Instantly
Weak	3 weeks
Strong	1 trillion years
Very Strong	500 quadrillion years
Strong	1 trillion years

The table above summarizes the assessment results. Screenshots illustrating these outcomes are provided on the following pages.

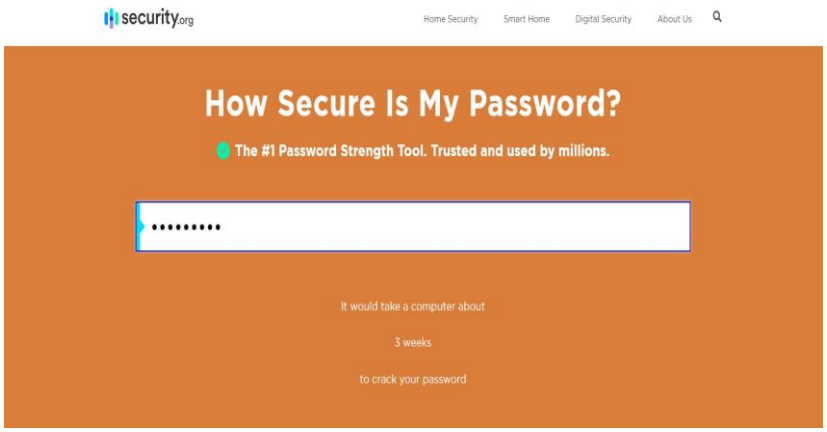
Screenshot 1

Very Weak Instantly - hello123

Screenshot 2

Weak 3 weeks –

Hello@123

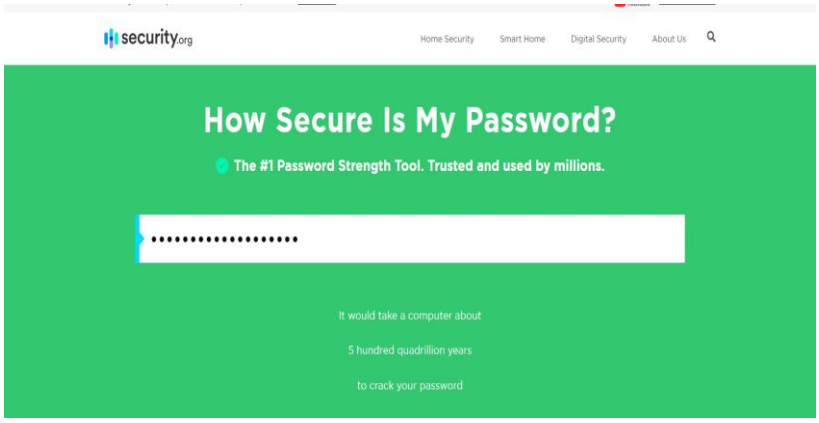


Screenshot 3

Strong - H3ll0_W0rld!2024

Screenshot 4

Very Strong - M!nD^P@$$_P0w3r#007



Screenshot 5

Strong - SkyIsTheL1mit!$#

3.Theoretical Background

3.1 Common Password Attacks

a) Brute-Force Attack: A program systematically tries every possible character combination until it finds the correct password. Short or simple passwords succumb quickly, whereas long and complex passphrases are exponentially harder to crack.

b) Dictionary Attack: Rather than guessing every combination, attackers test passwords from a pre-compiled list of words, phrases, and leaked credentials. Users who rely on predictable patterns or real words are particularly vulnerable.

3.2 Importance of Password Complexity

- Length: Each additional character multiplies the search space.
- Variety: Mixing upper/lowercase letters, digits, and symbols broadens complexity.
- Unpredictability: Avoiding real words, personal data, or sequential patterns makes dictionary attacks ineffective.

3.3 Tools & Best Practices

Password Managers: Applications such as Bitwarden, 1Password, or KeePass securely generate and store unique passwords.

MultiFactor Authentication (MFA): Adds a second factor (OTP, biometric, hardware token) that blocks unauthorized access even if a password is compromised.

Passphrases: Long combinations of unrelated words (e.g., 'Tiger-Coffee-Moon-2025') balance memorability and strength.

3.4 Common Mistakes to Avoid

- Using default or easily guessed passwords like 'admin' or '123456'.
- Reusing the same password across multiple services.
- Choosing short passwords without character diversity.

Conclusion

By systematically testing passwords of varying complexity, I observed how a modest changesuch as adding symbols or increasing lengthshifts cracking estimates from minutes to trillions of years. This practical experiment reinforces textbook guidance: robust passwords combined with MFA and sound hygiene are vital to modern cyber defense.