Task 6 – Password Strength Evaluation Report

Objective

To understand what makes a password strong by creating multiple passwords of varying complexity, testing them using online tools, and interpreting how structure affects strength and security.

Methodology

1. Created five passwords with different complexity levels.
2. Tested each on three password strength checkers:
    - https://bitwarden.com/password-strength/
    - https://passwordmeter.com/
    - https://www.security.org/how-secure-is-my-password/
3. Compared scores and crack time estimates.
4. Derived best practices for strong password creation.

Passwords Tested

No.	Password	Type	Bitwarden Rating	Pasword Meter Rating	Estimated Crack Time (Security.org)	Observation
1	sunshine12	Weak	Very Weak (2 secs)	Weak (37%)	<1 day	Common word + short length + no symbols
2	SkyBlue2025	Moderate	Weak (2 days)	Strong (91%)	41 years	Includes mixed case + digits but still predictable
3	S!ky_Blue2025	Strong	Good (2 Years)	Very Strong (100%)	2 million years	Added symbol + underscore increased entropy
4	T!ger$Run_47#Fast	Very Strong	Strong (Centuries)	Very Strong (100%)	93 trillion years	Long, mixed, random pattern
5	!9AqX$7rZ&vLp#T2nK	Random Strong	Strong (Centuries)	Very Strong (100%)	7 quadrillion years	High entropy randomly generated string

Findings

- **Length matters**: every extra character exponentially increases crack time.
- **Character diversity** (uppercase, lowercase, numbers, symbols) improves entropy.
- **Avoid dictionary words** – they make passwords vulnerable to dictionary attacks.
- **Randomness** offers the highest security but reduces memorability.
- **Passphrases** (e.g., Coffee$Mountain!River_2025) balance strength and ease of recall.

Common Password Attacks

Attack Type	Description	Example
Brute Force	Tries all possible combinations until correct.	aaaa→zzzz
Dictionary Attack	Uses common word lists or phrases.	password, qwerty
Phishing	Tricks users into revealing credentials.	Fake login emails
Credential Stuffing	Reuses stolen credentials from other sites.	Leaked user/password reuse

Best Practices for Strong Passwords

1. Use at least 12–16 characters.
2. Combine uppercase, lowercase, numbers, and symbols.
3. Avoid personal information (names, dates).
4. Use unique passwords for each account.
5. Prefer **passphrases** that mix unrelated words.
6. Enable **multi-factor authentication (MFA)** wherever possible.
7. Store securely in a **password manager** like Bitwarden or 1Password.

Conclusion

The evaluation proves that password strength depends primarily on length, complexity, and randomness.
Short or predictable passwords fail instantly under brute-force tests, while well-constructed random passwords can resist cracking for millennia.
Implementing strong password habits and multi-factor authentication is essential for robust digital security.