Task 6 - Password Strength Evaluation

1. Methodology

1. Created 9 test passwords covering a range from very weak to very strong, including examples with personal information and common patterns.
2. Evaluated each password using:
   - Password Meter (passwordmeter.com)
   - zxcvbn demo (dropbox.github.io/zxcvbn)
3. Recorded:
   - Password ID and actual password text
   - Length
   - Character types used
   - Strength score/label
   - Entropy (if provided)
   - Estimated crack time (if provided)
   - Tool feedback/suggestions
4. Real passwords are shown here for documentation purposes only; when testing on public tools, dummy/test values or masked entries should be used to avoid exposure.

2. Password List

P1 | summer2020 | Very weak

P2 | Password123 | Weak

P3 | P@ssw0rd! | Common + symbol

P4 | G7!mN9z | Short strong

P5 | T#9v7Qp8L3rW | Long strong

P6 | correct-horse-battery-staple | Passphrase

P7 | sunflower river pizza 1987 | Long passphrase

P8 | qwerty!@# | Pattern-based (bad)

P9 | Anita1999@ | Personal info (bad)

3. Results Table

ID	Password	Len	Char types	Tool	Score/Label

P1	summer2020	10	lower+digits	PasswordMeter	52% (Good)
P2	Password123	11	mixed+digits	PasswordMeter	48% (Weak)
P3	P@ssw0rd!	9	mixed+symbol+digit	PasswordMeter	64% (Medium)
P4	G7!mN9z	7	mixed+symbol+digit	zxcvbn	Score 3/4 (Strong)
P5	T#9v7Qp8L3rW	12	all char types	zxcvbn	Score 4/4 (Strong)
P6	correct-horse-battery-staple	28	words+hyphens	zxcvbn	Score 4/4 (Strong)
P7	sunflower river pizza 1987	26	words+digits	zxcvbn	Score 4/4 (Strong)
P8	qwerty!@#	9	lower+symbols	PasswordMeter	42% (Weak)
P9	Anita1999@	10	mixed+digits+symbol	PasswordMeter	46% (Weak)

4. Analysis

- Length dramatically increases crack time - P5 and P6 outperform short strong passwords even with fewer special characters.
- Randomness and avoiding common patterns are essential - P3 shows that substitutions like '@' for 'a' are not enough.
- Passphrases (P6, P7) balance memorability with security if words are truly random.
- Personal info (P9) and keyboard patterns (P8) remain weak despite added symbols.

5. Best Practices

- Minimum 12 characters; longer if possible.
- Use random combinations or multiple random words.
- Avoid personal info, dictionary words, or patterns.
- Use a unique password for each account.
- Consider a password manager for generation and storage.
- Enable multi-factor authentication for critical accounts.