# Password Strength Evaluation Report

Date: 2025-09-30T22:11:28.884874Z

## Methodology

- Created a list of 10 sample passwords with varying length and complexity.

- Estimated character pool size by checking for presence of lowercase, uppercase, digits, symbols, and spaces.

- Calculated entropy using E = L \* log2(R).

- Penalized entropy by up to 10 bits if the password contained common dictionary words (heuristic to reflect reduced unpredictability).

- Converted entropy into estimated average crack times under different attacker rates (see scenarios).

## Scenarios used for time-to-crack estimates

- Online throttled attacker: 100 attempts/sec

- Moderately fast API or distributed bot: 10,000 attempts/sec

- Offline GPU cracking: 10^10 attempts/sec

- High-power cluster: 10^14 attempts/sec

## Key findings (top highlights)

- Strongest sample: `3xtra-long-passphrase-with-hyphens-and-words-2025` with ~299.32 bits of entropy.

- Weakest sample: `password123` with ~46.87 bits of entropy.

## Tips & Best Practices

1. Prefer long passphrases (use 3-5 random common words or more) — length increases entropy fast.

2. Avoid common dictionary words or predictable substitutions like 'P@ssw0rd' — attackers use dictionary+substitution lists.

3. Use a password manager to generate and store long random passwords (recommended for unique site passwords).

4. Allow spaces and special characters; longer is better than arbitrary complexity rules.

5. Use multi-factor authentication (MFA) wherever possible — it greatly reduces risk even if a password is compromised.

## Common Attacks (brief)

- Brute force: trying all possible combinations — time depends on entropy and attackers' compute power.

- Dictionary attack: tries common words, leaked passwords, and common substitutions — very effective against human-chosen passwords.

- Credential stuffing: reuse of breached username/password pairs across sites — mitigated by unique passwords per site.

## References & Tools

See OWASP and NIST guidance on password policies and storage for authoritative recommendations.

(Also consulted: passwordmeter.com for example strength heuristics, and articles on entropy calculations.)

---

A full CSV with detailed estimates is saved at `{csv\_path}`.