

Password	Score	Strength	Notes
12345678910	9%	Very Weak	Numeric only, predictable, sequential
abc123	32%	Weak	Short, common pattern, lacks complexity
P@ssw0rd	68%	Strong	Predictable but meets complexity criteria
A1b2C3d4	86%	Very Strong	Excellent mix of character types
Tm#92wPq%LkZ	100%	Very Strong	High entropy, secure against most attack vectors
correcthorsebatterystaple	25%	(Actually Strong)	Good length; weak rating due to lack of variety, but strong in practice

Best Practices for Strong Passwords

From evaluation results and standard guidelines:

- Use **12+ characters**
- Combine **uppercase, lowercase, numbers, and special characters**
- Avoid dictionary words or keyboard patterns
- Don't reuse old passwords
- Prefer **random strings or long passphrases**
- Change passwords regularly, especially after a breach

Common Password Attacks






Attack Type	Description
Brute Force	Attempts all possible combinations until successful.
Dictionary Attack	Uses a list of common passwords/phrases.
Credential Stuffing	Uses stolen credentials from other services.
Phishing	Tricks users into revealing passwords via fake websites or emails.

How Complexity Helps

Password complexity:

- Increases the time needed for brute-force attacks
- Makes dictionary attacks ineffective
- Prevents pattern-based predictions
- Combined with **MFA**, makes accounts much harder to compromise

Tips for Strong Password Management

-  Use **password managers** like Bitwarden, 1Password, or LastPass
-  Create **passphrases**: e.g., Sunlight&Moons@Night2025
-  Enable **multi-factor authentication (MFA)** wherever possible
-  Never reuse passwords across different accounts
-  Update important passwords every 3-6 months