Password Strength Checker Guide

Tool · Score Any Password Manually. Understand What Makes Passwords Hard To Crack.

A printable companion to the live Password Strength Checker. Use this guide to score any password yourself, understand the math behind cracking time, and learn the patterns attackers exploit.

How Password Strength Is Measured

Password strength is mostly about **entropy** — how unpredictable a password is. The more possible variations, the longer it takes to crack. Two factors drive entropy:

1. **Length** — every additional character multiplies the search space.
2. **Character pool** — using lowercase, uppercase, numbers, and symbols expands the search space at each character.

Entropy formula: **log■(pool_size ^ length)**. Higher = harder to crack.

Strength Score Card

Length	Pool	Entropy (bits)	Brute-force time	Verdict
8 chars	lowercase only (26)	≈37	Seconds	Catastrophic
8 chars	mixed (94)	≈53	Hours	Weak
12 chars	mixed (94)	≈79	Centuries	OK
16 chars	lowercase only	≈75	Decades	OK if unique
16 chars	mixed (94)	≈105	Heat death of universe	Strong
20+ chars	any mix	120+	Effectively uncrackable	Excellent

Cracking times assume modern offline attacks (~100 billion guesses/sec).

Score Your Own Password

Pick one of your important passwords. Check each row that applies.

- ☐ 16 or more characters long.
- ☐ Contains lowercase letters.
- ☐ Contains uppercase letters.
- ☐ Contains numbers.
- ☐ Contains symbols.
- ☐ Random — not a word, name, date, or pattern.
- ☐ Unique to this account (not reused anywhere).

- Generated by a password manager (not invented by me).

8 boxes ticked = strong password. 4-7 = improve. 0-3 = change today.

Patterns Attackers Exploit

- **Dictionary words** — even with character substitution (P@ssw0rd, $ecur1ty).
- **Names + dates** — your name, kid's name, anniversary, birthday.
- **Keyboard walks** — qwerty, asdfgh, 1qaz2wsx.
- **L33t-speak substitutions** — they're in every cracker's wordlist.
- **Service-name passwords** — gmail2024, facebook!, instaSecure.
- **Common phrases** — letmein, welcome, password, iloveyou.
- **Reuse** — even a strong password becomes worthless if reused on a breached site.

The Right Way Forward

1. Use a **password manager** to generate every password — no human-invented passwords.
2. Set the manager's generator to 16+ characters with mixed character types.
3. Enable **MFA** on every account that supports it. A leaked password is much less damaging when MFA is required.
4. Run the manager's **breach scan** monthly. Replace anything flagged.
5. Never share passwords via email, text, or chat — use the manager's secure-share feature.

Run The Live Tool

Test any password instantly: visit the on-site Password Strength Checker. Get a real-time score, entropy estimate, and improvement suggestions.