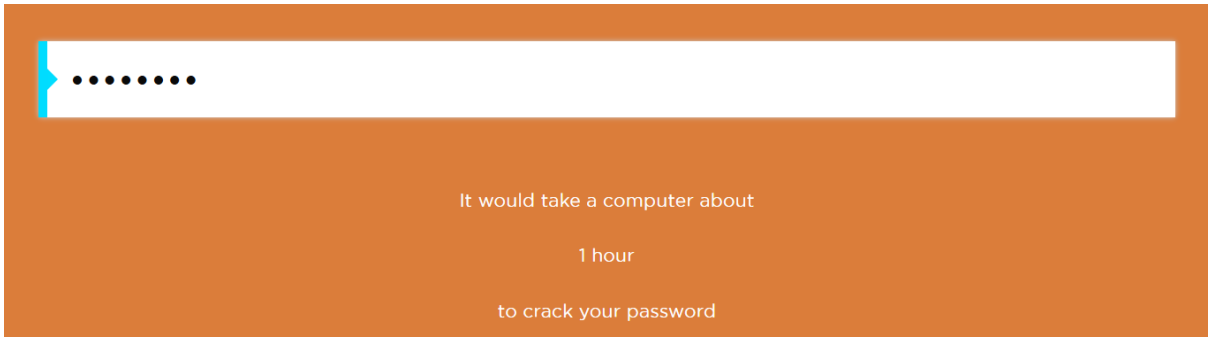
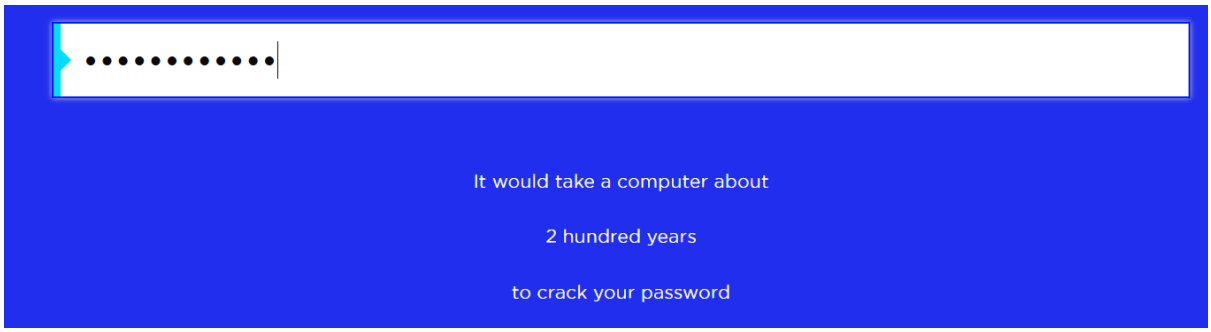
Results of Some Password Checks and their and feedback

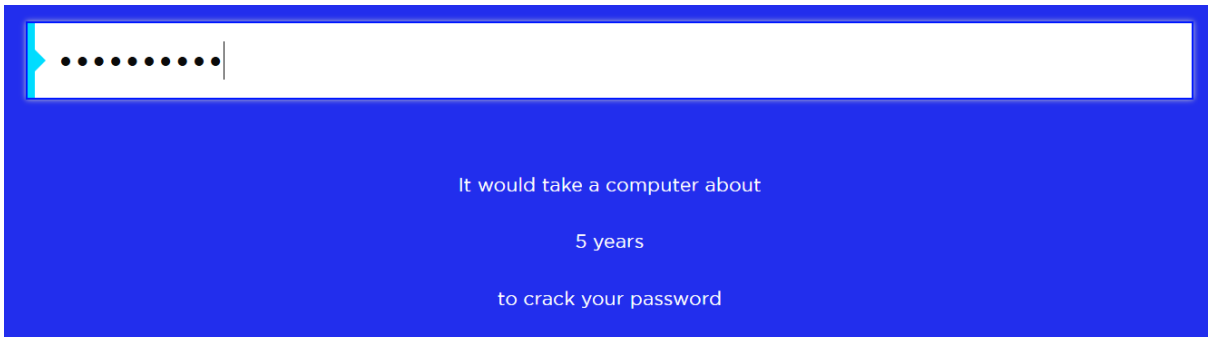
Pass1234



X9k@T3qLp*



letmein2024!



Types of Common Passwords Attacks

Attack	Description
Brute Force	Tries every possible combination; longer + complex passwords take more time
Dictionary Attack	Uses a list of common words and variations
Credential Stuffing	Uses leaked username/password combos
Phishing	Tricks users into revealing passwords via fake websites/emails
Keylogging	Malware records keystrokes to steal passwords

Identify Best Practices for Creating Strong Passwords

🔑 **Best Practices:**

1. Use at least **12 characters**
2. Include **uppercase**, **lowercase**, **numbers**, and **symbols**
3. Avoid **dictionary words**, **birthdays**, or **common phrases**
4. Don’t use **keyboard patterns** (e.g., qwerty, asdf)
5. Use **passphrases** with random or unusual words
6. Don’t reuse passwords across websites
7. Use a **password manager** to store complex passwords
8. Enable **two-factor authentication (2FA)** when possible