

## Results of Some Password Checks and their and feedback

Pass1234

A screenshot of a password strength checker interface. At the top, a white input field contains the password 'Pass1234', which is masked with 10 black dots. The input field has a blue arrow icon on its left side. Below the input field, the background is a solid orange color. Centered on this orange background is the text: 'It would take a computer about', '1 hour', and 'to crack your password'.

X9k@T3qLp\*

A screenshot of a password strength checker interface. At the top, a white input field contains the password 'X9k@T3qLp\*', which is masked with 10 black dots. The input field has a blue arrow icon on its left side. Below the input field, the background is a solid blue color. Centered on this blue background is the text: 'It would take a computer about', '2 hundred years', and 'to crack your password'.

letmein2024!

A screenshot of a password strength checker interface. At the top, a white input field contains the password 'letmein2024!', which is masked with 10 black dots. The input field has a blue arrow icon on its left side. Below the input field, the background is a solid blue color. Centered on this blue background is the text: 'It would take a computer about', '5 years', and 'to crack your password'.

### 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