Interview Questions – Simple & Clear Answers

1. What makes a password strong?

A strong password is long (12+ characters), includes uppercase, lowercase, numbers, and special symbols, and avoids using common words or personal information.

2. What are common password attacks?

Brute force, dictionary attack, credential stuffing, phishing, keylogging, and social engineering are common methods to crack or steal passwords.

3. Why is password length important?

Longer passwords are harder to crack because the number of possible combinations increases exponentially with each added character.

4. What is a dictionary attack?

It's a method where attackers try common words or leaked passwords from a wordlist to guess a password.

5. What is multi-factor authentication?

MFA adds an extra layer of security by requiring something you know (password) plus something you have (OTP, device) or are (fingerprint).

6. How do password managers help?

They generate and securely store strong, unique passwords for every account so you don't have to remember them all.

7. What are passphrases?

A passphrase is a string of unrelated words (e.g., `blue-mango!River2025`) that is easy to remember but hard to guess or crack.

8. What are common mistakes in password creation?

Using names, birthdays, common words like `123456`, short lengths, or reusing the same password across multiple sites.