1. What makes a password strong?

A strong password combines uppercase and lowercase letters, numbers, and special symbols. It should be at least 12 characters long and avoid easily guessed information like names or birthdates. Random and complex passwords are harder for attackers to crack.

2. What are common password attacks?

Common password attacks include brute-force attacks, dictionary attacks, and phishing. In these attacks, hackers try every possible combination or use common passwords to gain access. Social engineering and credential stuffing are also frequently used methods.

3. Why is password length important?

The longer a password is, the harder it becomes for attackers to guess or crack using brute-force methods. Each extra character increases the number of possible combinations exponentially. Hence, longer passwords provide stronger security protection.

4. What is a dictionary attack?

A dictionary attack uses a list of common words or passwords to try and guess a user's password. Attackers rely on predictable human behavior, such as using real words or simple patterns. Using random characters and phrases can help defend against such attacks.

5. What is multi-factor authentication?

Multi-factor authentication (MFA) adds an extra layer of security beyond just a password. It requires additional verification, like a fingerprint, security code, or mobile confirmation. This makes it much harder for hackers to access an account even if they know the password.

6. How do password managers help?

Password managers securely store and manage all your passwords in one encrypted location. They can generate strong, unique passwords for each account and fill them automatically. This reduces the risk of using weak or reused passwords across sites.

7. What are passphrases?

Passphrases are long combinations of random or meaningful words used instead of traditional passwords. They are easier to remember but still strong if they are lengthy and unique. For example, 'BlueSkyDance!River2025' is both strong and memorable.

8. What are common mistakes in password creation?

People often use simple, short, or easily guessed passwords like '123456' or 'password'. Reusing passwords across multiple accounts is another major mistake. Avoiding personal information and using random characters helps improve security.