1. What makes a password strong?
   Ans: A strong password is a complex combination of characters including uppercase and lowercase and special character. Randomness is key to making it resistant to attacks.

2. What are common password attacks?
   Ans: Brute- force Attacks, dictionary attacks, and Phishing

3. Why is password length important?
   Ans: Longer passwords provide more combinations, making them harder to crack which increases security.

4. What is a Dictionary Attack?
   Ans: It uses a list of common words, phrases, or leaked passwords to guess a user's credentials.

5. What is multi-factor authentication?
   Ans: It adds an extra layer of security by requiring users to provide two or more verifications factors to access an account.

6. How do password managers help?
   Ans: by securely storing and generating complex, unique passwords for each account.

7. What are passphrases?
   Ans: It is longer sequences of random words, often easier to remember but harder to guess.

8. What are common mistakes in password creation?
   Ans: Reusing passwords across accounts, repeating patterns, and not updating passwords regularly.