Password Security Guide

1. What makes a password strong?

A strong password is:

- Long - at least 12-16 characters.
- Complex - uses a mix of uppercase letters, lowercase letters, numbers, and symbols.
- Unpredictable - not based on personal information or common words.
- Unique - not reused across multiple accounts.

2. What are common password attacks?

- Brute-force attack - trying all possible combinations until the correct one is found.
- Dictionary attack - using a list of common words and passwords.
- Credential stuffing - using stolen credentials from other breaches.
- Phishing - tricking users into revealing passwords.
- Keylogging - capturing keystrokes to record passwords.

3. Why is password length important?

Longer passwords exponentially increase the number of possible combinations, making brute-force attacks much harder and slower. A 16-character password is vastly more secure than an 8-character one, even if both use mixed characters.

4. What is a dictionary attack?

A dictionary attack is a hacking method that uses a precompiled list (dictionary) of common words, passwords, and variations to guess a password quickly, instead of trying every possible combination like brute force.

5. What is multi-factor authentication (MFA)?

MFA adds extra layers of security beyond just a password. It usually involves:

- Something you know (password).
- Something you have (security token, phone).
- Something you are (fingerprint, face recognition).

This reduces the risk even if the password is compromised.

6. How do password managers help?

Password managers store and encrypt all your passwords in one secure vault, allowing you to:

- Use unique, complex passwords for each account.
- Avoid remembering multiple passwords.

- Auto-fill login credentials securely.

7. What are passphrases?

A passphrase is a longer sequence of words or a sentence used as a password. Example: "BlueTiger!JumpsOver7Hills". They are easier to remember yet harder to crack because of their length.

8. What are common mistakes in password creation?

- Using short passwords.
- Using personal details like names or birthdays.
- Reusing passwords across sites.
- Using common words or patterns like '123456' or 'password'.
- Failing to update passwords after a breach.