Password Security Tips & Key Concepts

What Makes a Password Strong?

- Use at least 12 characters
- Include uppercase, lowercase, numbers, and symbols
- Avoid personal info like names or birthdates
- Do not use dictionary words or common patterns

Common Password Attacks:

1. Brute Force Attack:

- Attempts every possible combination until the password is found.

2. Dictionary Attack:

- Tries commonly used words and passwords from precompiled lists.

Why Password Length is Important:

- The longer the password, the harder it is to crack.
- 16+ characters is recommended for maximum safety.

What is a Passphrase?

- A series of unrelated words like "Purple$Tiger!Rides7Moon"
- Easier to remember but still highly secure

Multi-Factor Authentication (MFA):

- Adds a second layer of security (e.g., OTP, biometrics)
- Even if password is compromised, access is blocked without 2nd factor

Password Managers:

- Generate and store complex passwords securely

- Reduce the risk of reusing or forgetting passwords

Common Mistakes in Password Creation:

- Using predictable words or sequences (e.g., "123456", "qwerty")

- Reusing passwords across multiple accounts

- Using personal info like pet names, birthdays, or favorite teams