Research: Common Password Attacks

1. Brute Force Attack

A brute force attack is a method where the attacker systematically tries all possible combinations of characters until the correct password is found.

How It Works:

- Automated tools try every possible password.
- Starts with simple combinations like 'a', 'aa', 'aaa', etc.

Why It's Dangerous:

- Guarantees a correct guess with enough time and power.
- Short or simple passwords are cracked quickly.

How to Protect:

- Use longer passwords (12+ characters).
- Include special characters, numbers, and mixed case.
- Enable account lockout after multiple failed attempts.
- Use multi-factor authentication (MFA).

2. Dictionary Attack

A dictionary attack uses a precompiled list of common words and passwords to guess a user's password.

How It Works:

- The attacker loads a 'dictionary file' with:
  - Real words (e.g., 'sunflower', 'computer')

Research: Common Password Attacks

- Common passwords (e.g., '123456', 'qwerty')

- The tool tries each entry until it finds a match.

Why It's Effective:

- Many people use simple or reused passwords.

- Faster than brute force because it tries likely options.

How to Protect:

- Avoid real words or predictable patterns.

- Don't use names, birthdays, or keyboard patterns.

- Use random passphrases (e.g., 'Yellow!Tiger@92Run').

Summary Table

```
Attack Type       | Description                         | Risk Level | Protection Methods
------------------|-------------------------------------|------------|-------------------
--
Brute Force         | Tries all possible combinations     | High         | Long, complex
passwords + MFA
Dictionary Attack | Tries common passwords/words        | High        | Unpredictable and
unique passwords
```