1.

1. apple123 – very simple
2. MangoTree – a little better, but still weak
3. Dog#2025 – stronger, has a symbol and number
4. 9!tZ@vQ3 – very strong and random
5. sunshine – weak, common word
6. G!8dK9$zL4w – very strong, long and mixed

   All the above password has uppercase,lowercase,numbers,symbols, And length variation.

2.

I used a standard password strength checker like Kaspersky

Password	**Strength**
apple123	Very Weak
MangoTree	Weak
Dog#2025	Strong
9!tZ@vQ3	Very Strong
sunshine	Very Weak
G!8dK9$zL4w	Extremely Strong

3. Notes from the Tool

- Short and simple passwords are easy to break
- Long and random passwords are very secure
- Symbols and numbers make passwords stronger
- Avoid using real words like “sunshine”

4.

Tips for Strong Passwords

- Use at least 10–12 characters

- Mix uppercase, lowercase, numbers, and symbols
- Don’t use names, birthdays, or simple words
- Don’t reuse passwords for different websites
- Try a password manager to remember strong passwords

5. I learned

- Longer passwords are harder to hack
- Random characters are better than real words
- Simple passwords like apple123 are too risky
- Always include symbols and numbers
- Password checkers help you see how strong your password is

6.

Common Ways Hackers Try to Break Passwords

- Brute Force Attack: Tries all possible combinations
- Dictionary Attack: Uses common words and passwords
- Phishing: Tricks you into giving your password
- Keylogging: Records what you type to steal passwords

7. Importance of strong password

If your password is simple, hackers can break it in seconds.
If your password is complex and long, it might take 100 years or more to break.
So, more complexity = more safety.