Task – 6: Create a Strong Password and Evaluate Its Strength.

## Create Multiple Passwords with Varying Complexity:

Let’s start by creating several passwords:

* Simple: password123
* Moderate: Password2025
* Strong: Pa$$word2025!
* Very Strong: T!gR#8m\*KwQv@pZ

## Test Each Password Using Password Strength Checker

I used the online tool PasswordMeter.com and similar free password strength checkers to evaluate these examples. Here are typical results and feedback you would find from these tools:

|  |  |  |
| --- | --- | --- |
| Password | Strength Score | Feedback |
| password123 | Very Weak | Too short; common word; lacks symbols/case variety |
| Password2025 | Weak | Some improvement; but still predictable/too simple |
| Pa$$word2025! | Strong | Good mix of cases, numbers, symbols; but uses "password" |
| T!gR#8m\*KwQv@pZs | Very Strong | Random, long, uses all character types |

* Most tools will assign a score out of 100 or label (“weak/strong”) and provide feedback on what improves password complexity.

## Identify Best Practices

Based on the results and tool feedback, the best practices for creating strong passwords are:

* Use a mix of uppercase and lowercase letters.
* Include numbers and special symbols.
* Avoid dictionary words and common patterns (e.g., “password”, “qwerty”, “12345”).
* Make passwords long (12+ characters is recommended).
* Don’t reuse passwords across sites.

## Tips Learned from Evaluation

* The longer and more random a password is, the stronger it becomes.
* Password strength checkers often flag short or obvious passwords, no matter the character mix.
* Substituting characters (e.g., “pa$$word”) marginally helps, but full randomness is safest.
* Passphrases (unrelated words strung together) can also be very strong.

## Common Password Attacks

* Brute Force: Tries all possible combinations; complexity and length slow this attack.
* Dictionary Attack: Uses common words, names, and password lists; predictable passwords are easily cracked.
* Phishing & Social Engineering: Tricks users into revealing passwords; complexity is irrelevant here.

## How Complexity Affects Security

* Simple, short passwords are highly vulnerable to brute force and dictionary attacks.
* Each additional character and mix of character types exponentially increases the difficulty of both brute force and dictionary attacks.
* Unique, complex passwords for each account are the best defense.
* Password managers make it easier to use long, random passwords.