# TASK 6

Create a Strong Password and Evaluate Its Strength

JUNE 3, 2025

PRADEEP U S

## Multiple Passwords

1. Simple password: password123
2. Medium password: Password2025
3. Strong password: P@ssw0rd2025!
4. Very strong password: 9x!P$Z@uR#bF1&cL
5. Weak password with symbols: hello!@#
6. Long passphrase: MyDogLoves2ChaseCats!

Used a Password Strength Checker

## Result table

| **Password** | **Score (%)** | **Crack Time** | **Feedback** |
|---|---|---|---|
| password123 | 20% | Less than 1 second | Too common, lacks complexity |
| Password2025 | 50% | Few seconds | Better, but still guessable |
| P@ssw0rd2025! | 75% | Few hours | Strong mix, but common base word |
| 9x!P$Z@uR#bF1&cL | 100% | Trillions of years | Excellent complexity and randomness |
| hello!@# | 25% | Less than a minute | Short, lacks numbers and uppercase |
| MyDogLoves2ChaseCats! | 90% | Centuries | Long and memorable phrase |

## Identify Best Practices

- Use **a mix of uppercase, lowercase, numbers, and special characters**.
- **Longer passwords** are exponentially stronger.
- Avoid **common words, dictionary terms**, or **personal info**.
- **Passphrases** (e.g., MyCatEats3FishDaily!) are secure and easier to remember.
- **Randomness and uniqueness** are key.

## Common Attacks

| **Attack Type** | **Description** |
|---|---|
| Brute Force | Tries every possible combination until it cracks your password. Longer and more complex passwords resist this better. |
| Dictionary Attack | Tries passwords from a predefined list of common passwords and words. Avoid using simple or predictable patterns. |
| Credential Stuffing | Uses leaked usernames/passwords from breaches to try logging in elsewhere. Use unique passwords per site. |

## Conclusion

Strong, unique, and complex passwords dramatically improve security against common password attacks. Users should leverage password managers to maintain multiple secure passwords.