**Title: Password Strength Checking Using Online Tools**

**Submitted by: Jingar Vishal Praveenkumar**

**Date: 6/6/25**

**Objective**

The aim of this task is to evaluate the strength of different passwords using an online tool called "Password Checker" and to understand the importance of strong passwords in ensuring online security. This document outlines the findings, weaknesses identified, and best practices for creating stronger passwords.

**Tools Used**

* **Password Checker** (online tool): This tool assesses password strength based on complexity, length, and common usage patterns.

**Procedure**

1. Multiple sample passwords were entered into the Password Checker tool.
2. The tool provided ratings (e.g., Weak, Medium, Strong) based on criteria such as length, use of special characters, common patterns, and dictionary words.
3. Weak passwords were analyzed to understand their shortcomings.
4. Suggestions were noted for improving password security.

**Examples of Passwords Tested**

| **Password** | **Strength** | **Weaknesses** |
| --- | --- | --- |
| 1234567890 | Very Weak | Common, short, no special characters |
| Abcd1234 | Very Weak | Dictionary word, numbers |
| qwerty123 | Weak | Keyboard pattern, easy to guess |
| Vishal@0906 | Medium | Capital + digits + special character |
| Iqwwd@10155 | Strong | Includes special characters, mixed case, and length |

**Analysis of Weak Passwords**

* **Too short**: Short passwords are easier to brute-force.
* **Common patterns**: Sequences or repeated characters are easily guessed.
* **No variety**: Lack of uppercase letters, digits, and symbols.
* **Dictionary words**: Easily cracked using dictionary attacks.

**Importance of a Strong Password**

* Prevents unauthorized access to personal and professional accounts.
* Protects sensitive data from cyber threats.
* Reduces the risk of identity theft and financial loss.
* Acts as a frontline defense against phishing and brute-force attacks.