**Title: Password Strength Testing and Evaluation**

**1. Objective**  
The objective of this activity is to understand what makes a password strong, test different passwords using an online password strength checker, and identify best practices for secure password creation.

**2. Tool Used**

* **Website:** [PasswordMeter.com](https://passwordmeter.com)
* **Function:** Evaluates passwords based on length, variety of characters (uppercase, lowercase, numbers, symbols), and common weakness patterns, then provides a score and complexity rating.

**3. Steps Taken**

1. Selected the online tool **PasswordMeter.com**.
2. Created three different passwords with varying complexity:
   * Weak (only lowercase letters)
   * Medium (letters + numbers)
   * Strong (letters + numbers + symbols + mixed case)
3. Entered each password into the tool and recorded:
   * Score (percentage)
   * Complexity rating
   * Tool feedback (strengths & weaknesses)
4. Took screenshots of the results for documentation.

**4. Results**

**1. Password: password123**

* **Score:** 43%
* **Complexity:** Good
* **Strength Factors (Additions):**
  + Number of Characters: 11 → **+44**
  + Lowercase Letters: 8 → **+6**
  + Numbers: 3 → **+12**
  + Middle Numbers or Symbols: 2 → **+4**
* **Weaknesses (Deductions):**
  + No Uppercase Letters → **0**
  + No Symbols → **0**
  + Consecutive Lowercase Letters: 7 → **-14**
  + Consecutive Numbers: 2 → **-4**
  + Repeat Characters: **-2**
  + Failed to meet all "Requirements" criteria (0 bonus)
* **Overall Assessment:**  
  This password is too simple and predictable. Lack of uppercase letters, symbols, and high consecutive character sequences make it vulnerable to brute-force and dictionary attacks.

**2. Password: T#9zQI5uR@1pL7xB**

* **Score:** 100%
* **Complexity:** Very Strong
* **Strength Factors (Additions):**
  + Number of Characters: 16 → **+64**
  + Uppercase Letters: 5 → **+22**
  + Lowercase Letters: 4 → **+24**
  + Numbers: 4 → **+16**
  + Symbols: 3 → **+18**
  + Middle Numbers/Symbols: 7 → **+14**
  + Met all "Requirements": 5 → **+10**
* **Weaknesses (Deductions):**
  + None (all deductions scored 0)
* **Overall Assessment:**  
  This password is extremely secure due to its long length, balanced use of uppercase, lowercase, numbers, and symbols, and lack of predictable patterns. It is resistant to most cracking techniques.

**3. Password: P@ssw0rd2025**

* **Score:** 100%
* **Complexity:** Very Strong
* **Strength Factors (Additions):**
  + Number of Characters: 13 → **+52**
  + Uppercase Letters: 1 → **+24**
  + Lowercase Letters: 5 → **+16**
  + Numbers: 5 → **+20**
  + Symbols: 2 → **+12**
  + Middle Numbers/Symbols: 6 → **+12**
  + Met all "Requirements": 5 → **+10**
* **Weaknesses (Deductions):**
  + Repeat Characters: **-2**
  + Consecutive Lowercase Letters: 3 → **-6**
  + Consecutive Numbers: 3 → **-6**
* **Overall Assessment:**  
  While this password is rated “Very Strong” and meets all major criteria, it contains recognizable dictionary elements (“Password” with substitutions) and predictable year format (“2025”). This may slightly reduce real-world security against targeted attacks.

**Comparison Table**

| **Password** | **Score** | **Complexity** | **Pros** | **Cons** |
| --- | --- | --- | --- | --- |
| password123 | 43% | Good | Meets length, has numbers | No uppercase, no symbols, predictable word, many consecutive characters |
| T#9zQI5uR@1pL7xB | 100% | Very Strong | Long, high entropy, full mix of char types | Hard to remember |
| P@ssw0rd2025 | 100% | Very Strong | Good mix of char types, easy to remember | Contains dictionary word, predictable date, some repetition |

**Recommendations**

1. **Avoid dictionary words** even with letter substitutions (e.g., “P@ssw0rd” is still guessable).
2. **Include all four character types** (uppercase, lowercase, numbers, symbols).
3. **Increase length**—ideally 14+ characters for maximum resistance to brute-force attacks.
4. **Avoid sequential patterns** or predictable numbers (e.g., years).
5. For very strong passwords like T#9zQI5uR@1pL7xB, consider using a **password manager** to store them securely.

**5. Analysis & Best Practices Learned**

* Longer passwords generally have higher strength scores.
* Mixing uppercase, lowercase, numbers, and special symbols significantly increases security.
* Avoid consecutive letters/numbers and dictionary words to prevent easy guessing.
* Passwords like P@ssw0rd!2025 scored higher because they combine length, character variety, and complexity.

**6. Common Password Attacks**

* **Brute Force:** Tries all possible combinations until the correct one is found. Longer and more complex passwords reduce feasibility.
* **Dictionary Attack:** Uses common words/phrases; avoid real words in passwords.
* **Credential Stuffing:** Uses leaked username-password pairs from other breaches; avoid reusing passwords.

**7. Conclusion**  
The evaluation confirmed that password strength is influenced by **length**, **character diversity**, and **randomness**. Following best practices can greatly reduce the risk of account compromise.