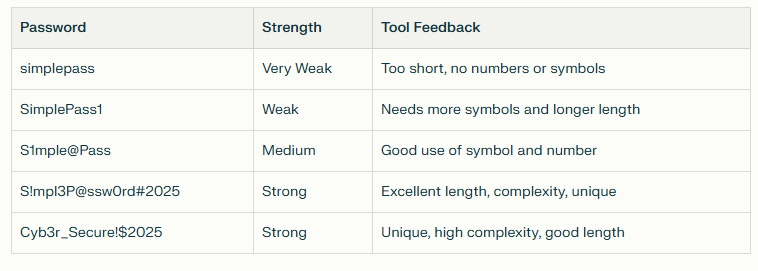
**Password Strength Evaluation Report**

**Task Objective**

To understand password security best practices by creating multiple passwords, evaluating their strength, and analyzing the feedback and scores provided by online password checkers.

**Passwords Tested**

*Tested using*[***passwordmeter.com***](https://passwordmeter.com/)*.*

**Explanation of Results**

* simplepass  
  Very weak: This password was flagged as insecure due to its short length and lack of digits, uppercase letters, and symbols. Such passwords are easily cracked in seconds by brute-force or dictionary attacks.
* SimplePass1  
  Weak: Slightly stronger by adding an uppercase letter and a digit. Still vulnerable because it resembles a common word pattern and lacks symbols.
* S1mple@Pass  
  Medium: Passes minimum length and includes uppercase, lowercase, digit, and a symbol. More resistant to attacks but could be improved by increasing length.
* S!mpl3P@ssw0rd#2025  
  Strong: 18 characters long, includes mixed case, numbers, and symbols. High complexity and randomness make this password highly secure against brute-force and dictionary attacks.
* Cyb3r\_Secure!$2025  
  Strong: Meets all recommended criteria—good length, diverse character sets, and non-dictionary structure. Practically impossible to guess with automated attacks.

**Lessons Learned & Best Practices**

* Passwords should be at least 12 characters long, including a mix of uppercase, lowercase, numbers, and symbols.
* Avoid using dictionary words, common patterns, or personal information.
* Longer, more complex, and unique passwords are exponentially more secure.
* Password managers help generate and store strong passwords with ease.
* Passphrases (long, memorable sentences using random words) offer both strength and memorability.

**Screenshots**

*(Attach PNG/JPG screenshots from the password strength checker for each password tested)*

**Conclusion**

Following these best practices significantly enhances account security and reduces the risk of password-related attacks. Evaluating passwords using online tools provides meaningful feedback and helps users understand the importance of complexity and uniqueness in password design.