* **Objective:** Create and test passwords of varying complexity using online password strength checkers.
* **Passwords Tested**

| **Password** | **Leaked in Database?** | **Tool Feeback** |
| --- | --- | --- |
| password123 | ✅ Yes (864,904 times) | Weak – lacks special characters, uppercase letters, and sufficient length. |
| Password@123 | ✅ Yes (1,064,154 times) | Weak – lacks sufficient length. |
| !P@y5W0rD2025! | ❌ No | Moderate – not leaked but still lacks length. |
| Th1s1sA$tr0ng#P@ss | ❌ No | ✅ Strong – complex, not found in leaks. |

* **Analysis & Observations**
* **Passwords found in leaked databases** are considered highly unsafe, even if they contain mixed characters.
* **Length** is critical. Even complex passwords may be flagged if too short.
* A **strong password** typically includes:
  + At least 12 characters
  + A mix of uppercase and lowercase letters
  + Numbers
  + Special symbols
  + Unpredictable structure (non-dictionary based)
* **Common Password Attacks**

1. **Brute-force attacks** – Tries all possible combinations.
2. **Dictionary attacks** – Uses common or leaked passwords.
3. **Credential stuffing** – Uses previously leaked username-password combos.
4. **Phishing** – Trick users into revealing passwords via fake websites.
5. **Keyloggers** – Malware records keystrokes.

* **Tips for Creating Strong Passwords**
* Use a **minimum of 12 characters**.
* Include **upper/lowercase letters, digits, and special characters**.
* Avoid using real words, names, or repeated patterns.
* Never reuse passwords across different accounts.
* Use a **password manager** to store and generate strong passwords.
* **Tool Used**
* **Website**: https://password.kaspersky.com