## Task 6 : Create a Strong Password and Evaluate Its Strength

Objective: Understand what makes a password strong and test it against password strength tools.
Tools: Online free password strength checkers (e.g., passwordmeter.com).
Deliverables: Report showing password strength results and explanation.

## Password Strength Evaluation Report

**Objective:**
To understand what makes a password strong and test password effectiveness using online strength checkers.

**Tools Used:**

- passwordmonster.com
- Kaspersky Password Checker
- NordPass Strength Checker

**Step 1–3: Created Passwords with Varying Complexity & Tested on Tools**

| Password | Length | Elements Used | Score (%) | Tool Feedback |
|---|---|---|---|---|
| hello123 | 8 | Lowercase + Numbers | 40% | Too short, predictable, lacks complexity |
| Hello123 | 8 | Upper + Lower + Numbers | 55% | Better, but still common and short |
| H3ll0@2024 | 10 | Upper + Lower + Numbers + Symbols | 85% | Strong, hard to guess |
| H@rD2Br3@k!# | 12 | All types + Length | 95% | Very strong, not dictionary-based |
| qwerty123 | 9 | Common pattern | 25% | Easily cracked, common sequence |
| Tr0ub4dor&3 | 11 | Mixed + Substitutions | 90% | Complex and well-designed |

**Step 4: Notes on Tool Scores & Feedback**

- Tools penalize **short length**, **common phrases**, and **keyboard patterns** (e.g., qwerty).
- Rewards are given for:
    - **Length > 10 characters**
    - **Use of all character types**
    - **Unpredictable structure**
    - **Avoidance of dictionary words**

**Step 5: Best Practices Identified**

- Use **at least 12 characters**.
- Combine **uppercase, lowercase, numbers, and symbols**.
- Avoid **real words**, names, dates, and sequences.

- Use **passphrases** with complexity or **randomly generated** strings.
- Never **reuse passwords** across accounts.
- Consider a **password manager** for secure storage.

**Step 6: Tips Learned**

- Don't use simple substitutions alone (e.g., password → P@ssw0rd) — modern attackers anticipate this.
- Longer passwords exponentially increase security.
- Randomly generated passwords (e.g., hY!p9#LbWq@4) are highly secure.
- Passphrases (e.g., Dancing$Tacos_4Bears) are both memorable and strong.

**Step 7: Common Password Attacks**

| Attack Type | Description |
|---|---|
| **Brute Force** | Tries every possible combination until the correct one is found. Longer and more complex passwords slow this down drastically. |
| **Dictionary Attack** | Uses a list of common words or passwords (e.g., 123456, qwerty). Easily bypasses simple or reused passwords. |
| **Credential Stuffing** | Uses leaked username/password combos on multiple sites. Password reuse makes this effective. |
| **Phishing** | Tricks users into revealing passwords. Not impacted by complexity but underscores the need for multi-factor authentication. |

**Step 8: Summary – Password Complexity & Security**

- **Complexity directly correlates with resistance to attacks**. The more unique, longer, and randomized a password is, the harder it is to crack.
- **Simple passwords** can be broken in seconds with brute force or dictionary methods.
- **Strong passwords**, especially when combined with multi-factor authentication (MFA), significantly enhance account security.

**Conclusion**

Creating strong, unique, and complex passwords is a fundamental step in defending against cyber threats. Regularly updating passwords and using tools like password managers and MFA strengthens overall cybersecurity posture.