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

**Step 1 & 2: Create multiple passwords with varying complexity . Use uppercase, lowercase, numbers, symbols, and length variations**

* **Low Complexity (8-10 chars, simple mix):**

1. Summer2024
2. BlueCar99
3. Pizza1234

* **Medium Complexity (12 chars, mixed cases, numbers, some symbols):**  
  4. Sun$et2024!Xq  
  5. BlueCar#99xZ  
  6. P1zz@L0v3r!7
* **High Complexity (16 chars, full mix):**  
  7. 7S!mmer$94#XqLp  
  8. B!u3C@r99xZ&7pW  
  9. P!zz@L0v3r#04\*Q
* **Very High Complexity (20 chars, random mix):**  
  10. 9X!m$7Lp#QvZ&2RwYt3  
  11. B@7xZ!pW#9Lm&3VqRsY  
  12. P#2!zZ@L0v3r\*Qw8XpYt

**Step 3 & 4: Test each password on password strength checker. 4.Note scores and feedback from the tool**

| **No.** | **Password** | **Strength Score** | **Estimated Time to Crack** | **Feedback Summary** |
| --- | --- | --- | --- | --- |
| **1.** | Summer2024 | Weak | A few minutes | Common word + year; predictable pattern. |
| **2.** | BlueCar99 | Weak | A few minutes | Dictionary word + numbers; lacks complexity. |
| **3.** | Pizza1234 | Weak | A few minutes | Easily guessable; lacks special characters. |
| **4.** | Sun$et2024!Xq | Moderate | Several hours to days | Improved symbols and length. Still predictable. |
| **5.** | BlueCar#99xZ | Moderate | Several days | Better entropy; real words reduce uniqueness. |
| **6.** | P1zz@L0v3r!7 | Strong | Weeks to months | Good symbol/number substitution; good length. |
| **7.** | 7S!mmer$94#XqLp | Very Strong | Centuries | Complex mix, decent length, minimal patterns. |
| **8.** | B!u3C@r99xZ&7pW | Very Strong | Centuries | Excellent randomness and symbol variety. |
| **9.** | P!zz@L0v3r#04\*Q | Very Strong | Centuries | Secure symbol/number usage; no dictionary match. |
| **10.** | 9X!m$7Lp#QvZ&2RwYt3 | Extremely Strong | Trillions of years | Long, random, unpredictable. Excellent security. |
| **11.** | B@7xZ!pW#9Lm&3VqRsY | Extremely Strong | Trillions of years | Uncommon structure and full mix; highly secure. |
| **12.** | P#2!zZ@L0v3r\*Qw8XpYt | Extremely Strong | Trillions of years | Long with strong entropy and character variety. |

**Step 6: Tips Learned from Evaluation**

* Use a mix of uppercase, lowercase, numbers, and special characters.
* Increase password length; 12+ characters is recommended, 16+ is better.
* Password length significantly impacts strength more than just complexity.
* Simple dictionary words or common phrases drastically reduce password strength.
* Adding symbols and numbers improves strength but is not enough if the password is short or predictable.
* Very long passwords with diverse characters provide the best protection.
* Password strength checkers often consider known leaked passwords and common patterns.
* Using a password manager to generate and store complex passwords is highly recommended.

**Step 7: Research – Common Password Attacks**

* Understanding how attackers exploit weak passwords is essential for implementing secure authentication practices. Below are the most common types of password attacks:

**1. Brute Force Attack**

* **Description:** The attacker tries **every possible combination** of characters until the correct password is found.
* **Speed:** Depends on password length and complexity; short/simple passwords can be cracked in seconds.
* **Tools Used:** Hydra, John the Ripper, Hashcat.

**2. Dictionary Attack**

* **Description:** Uses a **predefined list of words**, phrases, and common passwords (e.g., 123456, password, let Mein).
* **Effectiveness:** High against users with weak or common passwords.
* **Tools Used:** Cain & Abel, Medusa, THC Hydra.

**4. Phishing Attacks**

* **Description:** Tricks users into **manually revealing** their passwords via fake websites or emails.
* **Prevention:**
  + Train users to **recognize phishing**.
  + Use **email filters** and **MFA**.
  + Regularly test employees with **simulated phishing**.

**5. Keylogging**

* **Description:** Malicious software records **keystrokes**, capturing the password as it's typed.
* **Prevention:**
  + Use **antivirus/anti-malware software**.
  + Keep OS and applications **patched and updated**.
  + Avoid installing software from **untrusted sources**.

**6. Man-in-the-Middle (MitM) Attack**

* **Description:** Intercepts data transmitted between a user and a server, potentially capturing login credentials.
* **Prevention:**
  + Use **HTTPS** with valid SSL/TLS certificates.
  + Avoid public Wi-Fi for sensitive logins without a **VPN**.

**Step 8: Summary – How Password Complexity Affects Security**

Password complexity directly impacts how secure an account is against both brute force and dictionary attacks.

*Stronger passwords = Longer cracking time = Higher resistance to attacks*

| **Complexity Factor** | **Impact on Security** |
| --- | --- |
| **Length** | Longer passwords exponentially increase difficulty. |
| **Character Variety** | Adding uppercase, lowercase, digits, and symbols expands the character space. |
| **Unpredictability** | Avoiding dictionary words and common patterns reduces susceptibility to guessing. |
| **Uniqueness** | Using different passwords per account prevents credential stuffing. |