**6.Write down tips learned from the evaluation**

**Password Evaluation Tips**

* **Longer passwords consistently score better:** Passwords above 12 characters earn "Very Strong" or "Exceptional" ratings and are harder to crack.
* **Mix of character types boosts strength:** Combining uppercase, lowercase, numbers, and symbols adds complexity and significantly increases the score.
* **Passphrases are highly effective:** Using phrases (e.g., "L4ur4L1k3sYuckyBurger5") results in stronger passwords that estimated to take centuries to crack.
* **Avoid dictionary words and common patterns:** Simple letter sequences or repeated characters (e.g., "ABCDEFGHIJKL") are rated "Very Weak" and are easy targets for brute-force attacks.
* **Middle placement of numbers/symbols helps:** Distributing numbers and symbols throughout the password (not just at the ends) increases strength.
* **No single character type only:** Passwords made of only letters or only numbers receive deductions and are much weaker.
* **Consecutive and sequential patterns weaken passwords:** Avoid using ordered strings of letters or numbers, as these patterns lower overall complexity and are penalized in scoring.
* **Each requirement met adds bonus points:** The more diversity in character types and placement, the higher the bonus and final score.

7.Research common password attacks (brute force, dictionary).

**Classic Password Attack Types**

| **Attack Type** | **How It Works** | **Defence** |
| --- | --- | --- |
| Brute-Force | Tries every possible combination until the password is found. | Long, complex passwords; login rate-limiting; MFA. |
| Dictionary | Tests passwords from a list of common or leaked words/phrases. | Avoid dictionary words; use unique passwords. |

**Advanced Password Attack Types**

| **Attack Type** | **How It Works** | **Defence** |
| --- | --- | --- |
| **Credential Stuffing** | **Uses stolen credentials from past breaches and tries them on multiple sites (targets password reuse).** | **Unique passwords per site; MFA.** |
| **Password Spraying** | **Tries a few common passwords (like "Welcome1") across many accounts to evade lockouts and detection.** | **Strong passwords, account lockout, MFA.** |
| **Phishing** | **Tricks users into entering their password on fake sites or via deceptive emails.** | **User awareness, anti-phishing tools, MFA.** |
| **Rainbow Table** | **Uses large, precomputed tables mapping hashes to passwords to crack hashed databases without real-time computation.** | **Salting hashes, strong hashing algorithms.** |

**Key Points for Defence**

* Always use unique passwords for every site and service.
* Make passwords long (at least 12–16 characters) and include uppercase, lowercase, numbers, and symbols.
* Use multi-factor authentication (MFA) wherever possible to add another security layer.
* Stay cautious of emails or messages asking for passwords and verify legitimate requests.
* Ensure password storage uses salted hash algorithms to prevent bulk hash reversal.

8. Summarize how password complexity affects security.

Think of your password like the lock on your front door—it’s there to keep the bad guys out and protect everything valuable inside. The trick to a good password is making it hard for others to guess, but still easy enough for you to remember.

Passwords that are longer and use a mix of big letters, small letters, numbers, and symbols are way tougher to crack. It’s like adding more bolts and deadbolts to your door. Short or simple passwords, like just using lowercase letters or “password123,” are like having a flimsy lock that a thief can pick in seconds.

The best approach is to create a password that’s both strong and memorable—maybe a fun phrase or a mix of words only you understand, sprinkled with some numbers and symbols for extra flair. This way, it’s not only secure but also something you won’t forget. And remember, never use the same password on different sites. Think of it like giving each door its own unique lock so if one door gets compromised, the rest stay safe.

Bottom line: aim for length, mix things up, and keep it unique. That’s your best defense in today’s digital world!