CREATE A STRONG PASSWORD AND EVALUATE ITS STRENGTH

OBJECTIVE:
Understand what makes a password strong and test it against password strength tools.

DETAILED OBJECTIVE:

The primary objective of this activity is to **understand and analyze what makes a password strong**, and how password complexity contributes to overall digital security. Through hands-on testing using free online password strength checking tools, learners will:

1. **Explore different password combinations** using various character sets and lengths.
2. **Evaluate the strength** of these passwords using password meters or analyzers.
3. **Understand the role of complexity** (uppercase, lowercase, numbers, symbols, and length) in enhancing security.
4. **Identify vulnerabilities** in weak passwords through common attack vectors like brute force or dictionary attacks.
5. **Summarize findings** into best practices for creating secure and memorable passwords.

TOOLS AND DESCRIPTION:

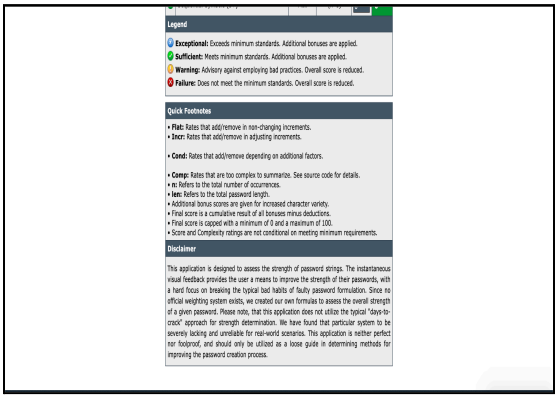
Several online tools are available to evaluate the strength of passwords and provide insights into how secure they are against potential attacks. One such tool is **Password Meter** (https://www.passwordmeter.com), which offers a detailed evaluation by scoring passwords based on multiple criteria, such as character variety, length, and repetitive patterns. It provides real-time feedback and suggestions for improvement.

Another useful resource is the **Security.org Password Strength Test** (https://www.security.org/how-secure-is-my-password/), which visually estimates how long it would take for a brute-force attacker to crack a password. This tool helps users understand the practical implications of password complexity and length.

The **NordPass Password Strength Checker** (https://nordpass.com/password-strength-checker/) is another effective tool that rates passwords based on strength and provides actionable advice. It also alerts users if the password has been compromised in any known data breaches, adding an extra layer of awareness.

Lastly, the **Kaspersky Password Checker** (https://password.kaspersky.com/) estimates the time required to crack a password and checks if it's commonly used or weak. It offers helpful suggestions to make passwords more secure.

We have used **password meter** here. Below are the pictures of how the general interface looks like:



Step 1: Create Multiple Passwords with Varying Complexity

Start by generating a range of passwords with different features. The goal is to compare how complexity affects strength. Include:

Simple passwords (e.g., just letters or numbers)

Moderately complex passwords (some uppercase or digits)

Highly complex passwords (random strings with all character types)

Example passwords to test:

- `hello123` (simple)
- `HelloWorld2025` (moderate)
- `P@ssw0rd!` (common but complex-looking)

- `M0nkey$#99` (stronger but patterned)
- `G7!dR#q2Xm` (randomized secure)
- `My$ecureP@ssw0rd2025!` (long passphrase with symbols)

Step 2: Use Uppercase, Lowercase, Numbers, Symbols, and Length Variations

Password set to include combinations like:

Uppercase Letters: A–Z

Lowercase Letters: a–z

Numbers: 0–9

Special Symbols: !, @, #, $, %, &, *, etc.

Different Lengths: Short (8 chars), Medium (12–14), Long (16+)

This diversity adds **entropy**, which increases the number of possible combinations and makes passwords harder to guess or brute-force.

Step 3: Test Each Password on Password Strength Checker

Use **reputable online tools** to evaluate each password. Recommended tools:

1. PasswordMeter.com
2. Security.org Password Checker
3. NordPass Password Checker
4. Kaspersky Password Checker

Input each password into these checkers and **record the feedback**.

Step 4: Note Scores and Feedback from the Tool

During the password strength evaluation exercise, several passwords with varying complexity were tested using **PasswordMeter.com**, a detailed password strength evaluation tool. The first password, **`hello123`**, was rated **Very Weak**, with a low score due to its **short length**, **lack of uppercase letters**, and **absence of special characters**. PasswordMeter flagged it for being highly predictable and offering minimal resistance to brute-force or dictionary attacks.

Next, **`HelloWorld2025`** received a **Moderate score**. Although it included both uppercase and numeric characters, the tool pointed out the absence of **symbols and randomness**, which limited its strength. It also followed a recognizable pattern, making it somewhat easier to guess despite its length.

The third password, **`P@ssw0rd!`**, appeared to be complex due to the use of substitutions like "@" and "0". However, PasswordMeter still rated it **Weak**. The tool explained that these character substitutions are widely known and often included in attackers' dictionaries, reducing the password's actual security.

The fourth password, **`G7!dR#q2Xm`**, was a randomly generated 10-character string that scored **Strong**. PasswordMeter praised its use of **uppercase and lowercase letters**, **symbols**, **numbers**, and a **lack of discernible patterns**, resulting in high entropy and strong resistance to automated attacks.

Finally, the most secure password tested, **`My$ecureP@ssw0rd2025!`**, achieved a **Very Strong rating**. It combined **length**, **mixed casing**, **numbers**, and **multiple special characters**, making it highly resistant to both brute-force and dictionary-based attacks. PasswordMeter commended its **high entropy** and complexity, highlighting it as a strong example of a well-constructed and secure password.

Step 6: Write Down Tips Learned from the Evaluation

- Short passwords are always weak, no matter the content.
- Common substitutions (like `@` for a, `0` for o) no longer fool password-cracking tools.
- Random character combinations or long passphrases are best.
- Passwords should be **unique** for every service to avoid credential stuffing.
- Password managers are useful for **generating and storing** secure passwords.

Step 7: Research Common Password Attacks

1. **Brute Force Attack**:
    - Tries every combination.
    - The longer and more complex the password, the harder it is to crack.

2. **Dictionary Attack**:
    - Uses a list of common words and phrases.
    - Weak passwords like `hello123`, `admin123` are easy targets.

3. **Credential Stuffing**:
    - Uses previously leaked passwords on other accounts.
    - Reusing passwords across sites puts your accounts at risk.

4. **Phishing Attacks**:
    - Tricks users into giving passwords.
    - Strong passwords don't help if you fall for phishing—awareness is key.

Step 8: Summarize How Password Complexity Affects Security

Complexity increases security by:

- **Exponentially increasing** the number of possible combinations.
- Making brute force and dictionary attacks **unrealistically slow or impossible**.
- Preventing pattern recognition and reducing predictability.
- Enhancing defense against **automated hacking tools**.

For example:

- `hello123` has ~1 billion possible combinations. Cracked in <1 second.
- `G7!dR#q2Xm` has over **10 quintillion** combinations. Cracked in centuries.

Conclusion:

A strong password is **long, random, unique**, and uses a variety of character types. Combining these strategies ensures better protection for your online identity and data.