🔐 Task 5. Creat a Strong Password and Evaluate its Strength

Topic: Password Security & Strength Evaluation

✅ Step 1: Create Multiple Passwords with Varying Complexity

Password	Description
`password123`	Common, weak password
`Pa$$w0rd!`	Medium complexity
`S@f3H0us3!2025`	Strong password with symbols, numbers
`Gk*83vd!j#L2`	Random, high complexity
`sunshine`	Simple dictionary word
`C0mpl3x_4#Us3r!`	Complex, user-friendly

✅ Step 2: Test Passwords Using a Password Strength Checker

You can use tools like:

- How Secure Is My Password
- Password Checker Online
- LastPass Password Generator

Record feedback and scores.

Password	Strength (Estimated)	Feedback
`password123`	Very Weak (Instant crack)	Common password, lacks complexity
`Pa$$w0rd!`	Weak (few minutes)	Better, but still predictable
`S@f3H0us3!2025`	Strong (millions of years)	Good length, variety of characters
`Gk*83vd!j#L2`	Very Strong (billions of years)	Random, very hard to crack
`sunshine`	Very Weak (instant crack)	Found in dictionary
`C0mpl3x_4#Us3r!`	Strong (billions of years)	Well-structured with symbols and length

✅ Step 3: Identify Best Practices for Creating Strong Passwords

From testing and research, best practices include:

- Use **12+ characters** (longer = stronger).
- Combine **uppercase, lowercase, numbers, and special characters**.
- Avoid **dictionary words** and common phrases.
- Don’t reuse passwords across sites.
- Use **passphrases** or randomly generated strings.
- Consider a **password manager** for storing complex passwords.

✓ Step 4: Tips Learned from Evaluation

- Even replacing letters with symbols (e.g., `Pa$$w0rd`) isn't enough if the base word is common.
- Truly secure passwords look random (e.g., `Gk*83vd!j#L2`).
- Adding length increases security more than just complexity.
- Mixing unrelated words (e.g., `BlueTable7!Rain`) can be both strong and memorable.

✓ Step 5: Research – Common Password Attacks

Attack Type	Description
Brute Force	Tries every possible combination until it finds a match.
Dictionary Attack	Uses known words/phrases from a list (like "password", "123456").
Credential Stuffing	Uses leaked credentials from data breaches.
Phishing	Tricks users into revealing passwords.
Keylogging	Captures typed passwords via malware.

✓ Step 6: Summary – How Password Complexity Affects Security

- **Low Complexity Passwords** (e.g., `password123`) are highly vulnerable to dictionary and brute-force attacks.
- **High Complexity Passwords** take **millions or billions of years** to crack using brute force, especially when long and random.
- Attackers rely on **common patterns** and **human laziness**—unique, complex passwords defend against this.
- The combination of **length + unpredictability** is the key to strong passwords.

Final Thoughts

Security Tip: Always use **multi-factor authentication (MFA)** alongside strong passwords for better protection.