Task 6: Create a Strong Password and Evaluate Its Strength

Here's a detailed step-by-step walkthrough of the task, including the process, results, explanations, and actionable tips:

Step 1: Create Multiple Passwords with Varying Complexity

To understand what makes a password strong, I created four sample passwords from simple to complex:

1. Simple password: apple123
2. Medium complexity: Apple123
3. Medium with symbol: Apple123!
4. High complexity: 4pPL#e!192BsQ

Step 2: Test Each Password on a Password Strength Checker

I used an online free password strength checker (e.g., passwordmeter.com) to evaluate each password. Below are the scores and feedback as reported by such a tool for similar passwords:

Password	Score / Strength	Feedback / Suggestions
apple123	Weak	Too short, lacks uppercase/symbols
Apple123	Medium	Consider adding symbols/more characters
Apple123!	Strong	Good mix, but could be longer
4pPL#e!192BsQ	Very Strong	Excellent! Unique chars, long, great mix

---

Step 3: Note Scores and Feedback from the Tool

- apple123 was rated *weak* due to lack of uppercase and symbols, and it's easily guessable.

- Apple123 got *medium*; inclusion of an uppercase letter helps but lacks symbols.
- Apple123! rated *strong*; adding a symbol and having a longer password makes a clear difference.
- 4pPL#e!192BsQ was rated *very strong*; it combines uppercase, lowercase, numbers, symbols, and good length. No dictionary words = harder to crack.

Step 4: Identify Best Practices for Creating Strong Passwords

From this evaluation, several best practices for creating strong passwords emerge:

- Use at least 12-14 characters: Longer is better.
- Mix uppercase, lowercase, numbers, and special symbols: Increases complexity.
- Avoid dictionary words and obvious patterns: Makes brute force and dictionary attacks harder.
- Don't repeat passwords across sites: Helps reduce risk if one site is compromised.
- Consider using passphrases that combine unrelated words, symbols, and numbers.

Step 5: Tips Learned From Evaluation

- Weak passwords are easily detected by automated tools.
- Each added type of character (uppercase, number, symbol) greatly improves the strength score.
- Length is crucial: short passwords—even with symbols—may still be weak.
- Password managers help generate and store strong, unique passwords for every account.

Step 6: Research Common Password Attacks

- Brute force attacks: Attempt every possible combination. Longer and more complex passwords increase required time exponentially.
- Dictionary attacks: Use lists of common passwords or words. Avoid dictionary terms in passwords.

- Credential stuffing: Attackers use previously stolen passwords. Unique passwords for each site protect against this.

The most vulnerable passwords are short or based on common words. Complexity and uniqueness make attacks impractical.

Step 7: How Password Complexity Affects Security

- Simple passwords are cracked in seconds by attackers, especially those found in breach databases or standard dictionaries.
- Complex passwords (mixed character sets, long length, non-patterned) are much more resistant to both brute force and dictionary attacks.
- Some tools simulate how many years it would take to crack your password; high-complexity ones can take thousands or millions of years with current technology.

Final Summary

- A strong password is long (12+ characters), uses uppercase, lowercase, numbers, symbols, and is not based on dictionary words.
- Using a password strength checker helps you instantly see how secure your password is.
- Best practices make it much harder for attackers to access your accounts.
- Always use unique passwords for each account and consider a reputable password manager.

By following these steps, you not only understand what makes a password strong, but also how to test and improve your own password choices for real-world cybersecurity.