Create a Strong Password and Evaluate Its Strength

1. Creating Multiple Passwords with Varying Complexity

Below are several example passwords, each with different complexity:

- Simple: password123
- Moderate: Summer2025!
- Strong: Br!ght&SunnyD@ys24
- Very Strong: ^Dr@g0n$&M@g1c^!

2. Testing Passwords on a Password Strength Checker

Using a tool like passwordmeter.com, here are typical results I find:

3. Best Practices for Creating Strong

Password	Length	Uppercase	Lowercase	Numbers	Symbols	Strength Score	Complexity
password123	11	0	8	3	0	43%	Good
Summer2025!	11	1	5	4	1	100%	Very Strong
Br!ght&SunnyD@ys24	18	3	10	2	3	100%	Very Strong
^Dr@g0n$&M@g1c^!	16	2	5	2	7	100%	Very Strong

Passwords

- **Use at least 12-14 characters**—longer is better.
- **Combine uppercase, lowercase, numbers, and symbols**.
- **Avoid dictionary words, names, or predictable patterns**.
- **Make passwords unique for every account**.
- **Use passphrases**—a memorable phrase with random words and symbols.
- **Password managers** can help generate and store strong, unique passwords for each site.

4. Tips Learned from Evaluation

- Passwords that are long, random, and contain a mix of character types are hardest to crack.
- Avoiding common words and patterns drastically improves security.
- Password strength checkers estimate how long it would take to crack your password, helping you make better choices.
- Using a password manager is safer than reusing or writing down passwords.

5. Common Password Attacks

- **Brute Force Attack:** Systematically tries every possible combination until the password is found.
- **Dictionary Attack:** Uses lists of common words and phrases, including variations, to guess passwords.
- **Credential Stuffing, Password Spraying, Phishing, Keylogging:** Other common attacks that exploit weak passwords or human behavior.

6. How Password Complexity Affects Security

- **Complex passwords** (long, random, mixed characters) are much harder and slower to crack, even with automated tools.
- **Simple passwords** or those based on dictionary words can be cracked in seconds or minutes using dictionary or brute force attacks.
- **Password length** exponentially increases the number of possible combinations, making brute force attacks far less effective.

7. Summary of Key Concepts

- **Password strength** is determined by length, complexity, and unpredictability.
- **Brute force and dictionary attacks** are major threats to weak passwords.
- **Best practices** include using long, unique, complex passwords and enabling multi-factor authentication.
- **Password managers** help generate and store strong passwords for every account.
- **Passphrases** (random words with symbols and numbers) are both strong and memorable.